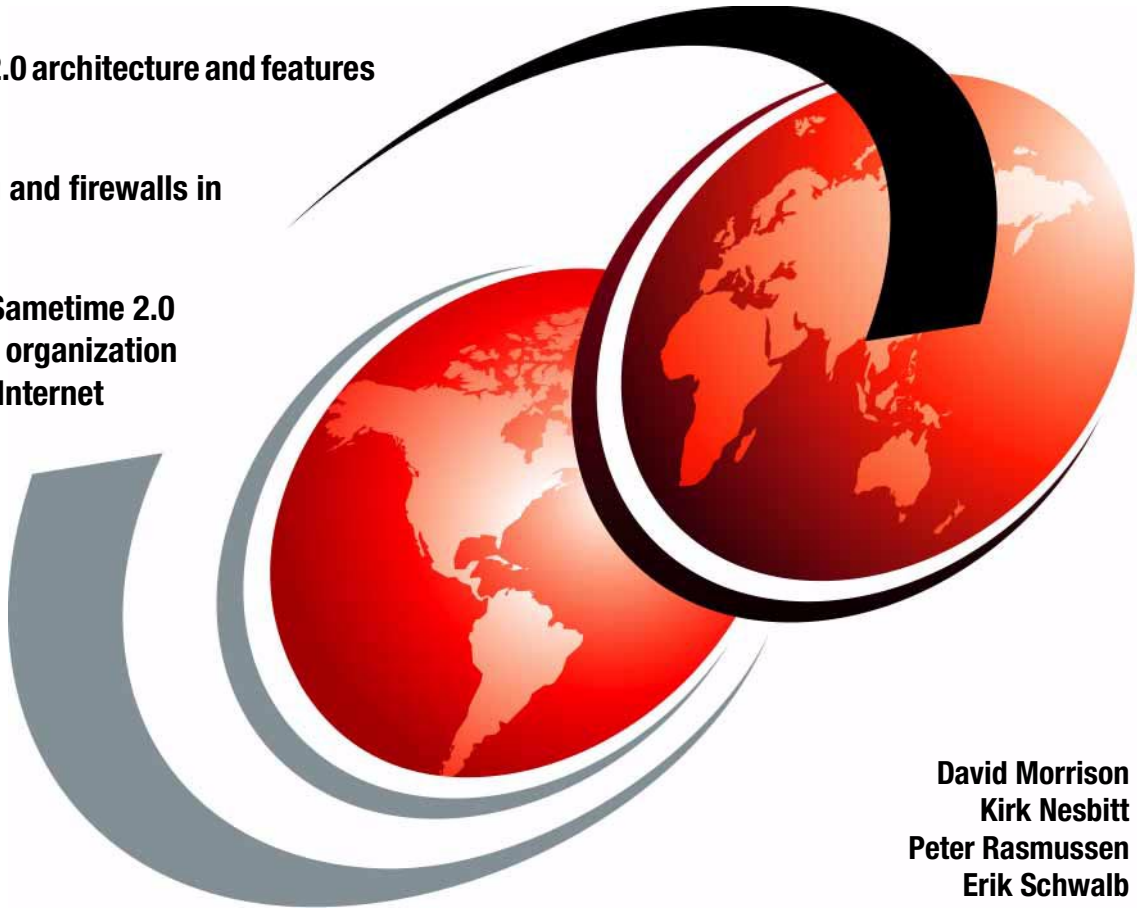
Lotus

IBM

Lotus Sametime 2.0 Deployment Guide

- Sametime 2.0 architecture and features
- Networking and firewalls in depth
- Deploying Sametime 2.0 within your organization and on the Internet



David Morrison
Kirk Nesbitt
Peter Rasmussen
Erik Schwalb

Redbooks

ibm.com/redbooks

SG24-6206-00

International Technical Support Organization

Lotus Sametime 2.0 Deployment Guide

February 2001

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, “Special notices” on page 177.

First Edition (February 2001)

This edition applies to Lotus Sametime 2.0 beta 2 for use on the Windows/32 platform.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. TQH 1CP-5605E
1 Charles Park
Cambridge, Massachusetts 02142-1245

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Preface

Efficient, flexible, instantaneous communication is critical to a company's success. Sametime supports immediate communication with people across the hall or around the world.

The Sametime family includes the Sametime Server, the Sametime Connect client, and a range of Application Developer Tools. The Sametime Server supports the T.120 standard and is designed to work smoothly with third-party clients like Microsoft's NetMeeting. The Sametime Server also works seamlessly with any browser or with Lotus Notes.

The Sametime product line supplies the three foundations of real-time collaboration: awareness, conversation, and shared objects.

Awareness means a member of a team is aware of when other members are online. You can share your awareness through Sametime Connect, a web page, or through a mobile device.

Conversations with others can easily be started using instant text messages or a chat session involving many people. With Sametime 2.0 you can also have audio/video sessions over IP.

Shared object capabilities enable team members to share live documents or applications with others. You can even permit others to control your screen, so you can collaborate on projects regardless of geographic distance. Lotus Sametime is a real-time collaboration tool that allows you to communicate with others instantly.

As a Sametime 2.0 deployer or network administrator, it is important for you to understand how the Sametime functions can be effectively used in your organization.

This redbook helps you install, tailor, and configure the new version of Sametime 2.0 to meet your business needs. It explains the installation options, deployment planning and implementation, and performance considerations. It then takes you under the covers of Sametime 2 and describes in detail what each of the services are, what they do, and how they work.

A detailed discussion of network issues, security concerns and firewall configuration helps you plan for deploying Sametime over the internet. Finally, we offer a real-world example of a Sametime implementation that connects users within the company, as well as to others on the Web.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Cambridge Center.

David Morrison is an International Technical Support Specialist for Lotus Notes and Domino at the International Technical Support Organization Center at Lotus Development, Cambridge, Massachusetts. He manages projects whose objective is to produce redbooks on all areas of Lotus products. Before joining the ITSO in 1999, he was a senior Lotus Notes consultant working for IBM e-business services in the United Kingdom.

Kirk Nesbitt is a Consultant for Lotus Professional Services in Sydney, Australia. He has 3 years of experience in Notes/Domino and website design and development. He holds a degree in Computer Science from the University of Technology in Sydney. His areas of expertise include website content management systems, Notes development and HTML/JavaScript.

Peter Rasmussen is currently an IT Advisor for IBM Global Services in the United States, working from his home in Orem, Utah. During his 5 years with IBM, he has worked extensively with users and PC systems within IBM, doing work in diverse areas such as Notes 4.0- 5.0, data backup, client migration, end-user support, and most recently, Sametime 1.5. Before joining IBM, Peter was an IBM client in AS/400 and PC systems operations. He holds a B.A. in International Relations, but has always worked with computers and the people that use them. His first experience with instant messaging was using "Call Sysop" on dial-up bulletin boards when 1200 baud modems were considered fast. This is his first published book.

Erik Schwalb is a Program Manager for Lotus Sametime, working for Lotus Development in Frankfurt, Germany. As a Senior System Engineer and Technology Manager for Lotus Central, he has 9 years of field experience with Lotus collaboration products. Besides Sametime, his areas of expertise include Notes and Domino architecture, Quickplace and Raven. Erik holds a degree in telecommunications and microprocessor electronics.

Thanks to the following people for their invaluable contributions to this project:

Brian Alyward, Wes Morgan, Bethann Cregg of Lotus Development

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Please send us your comments about this or other Redbooks in one of the following ways:

- Fax the evaluation form found in “IBM Redbooks review” on page 189 to the fax number shown on the form.
- Use the online evaluation form found at ibm.com/redbooks
- Send your comments in an Internet note to redbook@us.ibm.com

Chapter 1. Installation

This chapter describes the three installation options for Sametime server, various methods of distributing the Sametime Connect client to end users' machines, and the use of the Sametime client packager.

1.1 Sametime 2.0 Installation Options

There are three options for installing Sametime 2.0 in your organization:

- Installing Sametime on top of a Domino server
- Integrating a standalone Sametime server into an existing Domino domain
- A Web-only installation of Sametime

Each option will be explained in detail in the following sections.

Read This

This chapter will not provide step-by-step instructions for installation. Detailed installation instructions can be found in the installreadme.txt file that comes with the standard Sametime 2.0 Beta 2 distribution. You can obtain the latest version of this file from `www.lotus.com/sametime`.

1.1.1 Installing on top of an existing Domino Server

This section outlines mandatory pre-installation tasks and details some potential pitfalls associated with installing Sametime 2.0 on top of an existing Domino Server.

1.1.1.1 Why install Sametime 2.0 in this manner

When installed into a Domino environment, Sametime interacts with the Directory, security, and replication features of Domino servers.

Lotus recommends that the Sametime server be dedicated to supporting the real-time, interactive communication services of Sametime. A Sametime server should not be used for other high-demand Domino services such as mail storage and routing, application and database storage, or centralized Directory and administration services.

This option allows you to use a Domino Console and the Notes administration client to locally administer the server.

Larger sites will also benefit from not having to replicate the Domino Directory during the Sametime 2.0 installation process since a current copy will already exist on the server.

1.1.1.2 Pre-installation checklist

Ensure that you complete these mandatory pre-installation steps. Refer to the installreadme.txt file that is shipped with the Sametime 2.0 Beta 2 distribution for additional steps and background information prior to commencing installation.

- If you are installing Sametime 2.0 on Windows NT or Windows 2000, make sure that you disable Internet Information Server (IIS). Make sure that the service will not start on a subsequent reboot. Domino will be unable to start the HTTP task if IIS is running. The HTTP task must be running under Domino for Sametime to function.
- Ensure that your Domino Server is on release 5.0.3 or above. Sametime 2.0 requires the new design of the Domino directory available in Domino 5.0.3.
- Ensure that the administrator of the Domino server has an Internet password. You can do this by opening up the administrator's person document from the people view in the names.nsf database. Click on the Edit Person button and you should see something similar to Figure 1 on page 3. If the Internet Password field is blank, enter the password and save the document.

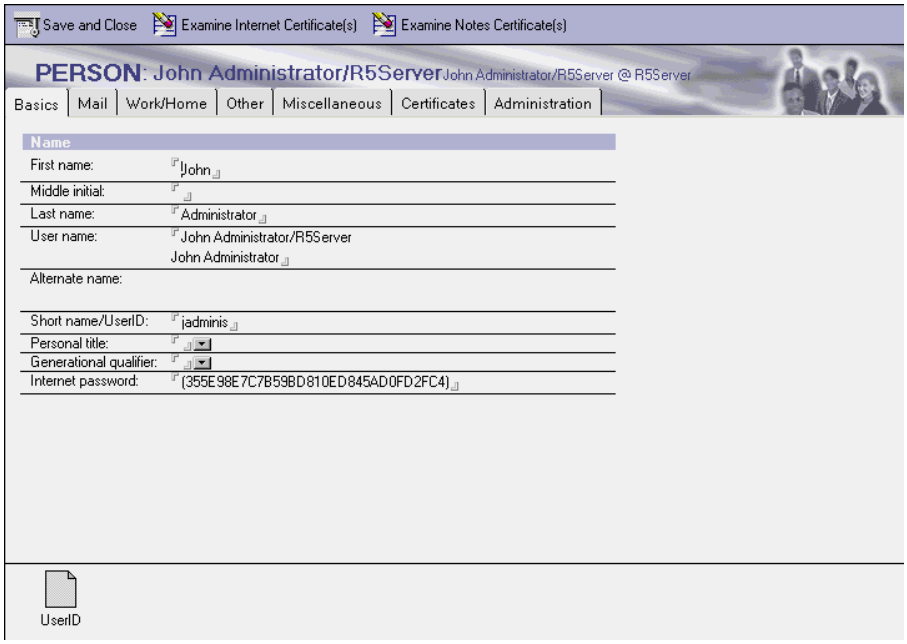


Figure 1. Person document with an Internet password specified

- Sametime uses agents that must access the Domino Directory. The minimal access level required for these agents is reader. Therefore, you should set the default ACL entry for the Domino Directory to Reader.
- If it is your organization's policy to maintain a No Access setting for the default entry of the Domino Directory, you must add the "Sametime Development/Lotus Notes Companion Products" ID to the ACL with a minimum access of Reader.
- Ensure that all applications on the target PC are shut down, including the Domino Server.
- If you will administer the Sametime Server via Internet Explorer, you must switch off HTTP 1.1. The administration client will not function correctly if HTTP 1.1 is enabled. refer to Section 1.2.4, "Disabling HTTP 1.1 support in Internet Explorer" on page 16. Netscape users will not have this problem, by default Netscape uses HTTP 1.0.

1.1.1.3 Directory considerations

When Sametime 2.0 is installed on top of a Domino server, the Domino Directory is used to store user details.

Each user in the Domino Directory that will use Sametime 2.0 will require an Internet password specified in their person document.

Specify the full canonical name of each user's home Sametime server in their person document. A simple agent can be used to perform this task.

Users are granted access to Sametime via basic Web authentication. Under basic Web authentication the password that the user specifies is compared to the password that exists in their person document. If the two passwords match, then the users is granted the access rights specified in the ACL of the database they are accessing.

The Directory can still be replicated with the Administration server via a replication schedule.

1.1.1.4 Potential pitfalls

Administrators should note that the default ACL setup of the Sametime Meeting center will allow full anonymous access via a Web browser. Details of securing the meeting center can be found in 1.2.2, "Securing the meeting room" . This means that any user in your organization that can access the Sametime Server via a Web browser can start and attend meetings under any name they choose. It may not be obvious to new users that this has happened. See Figure 2 on page 5 for an example.

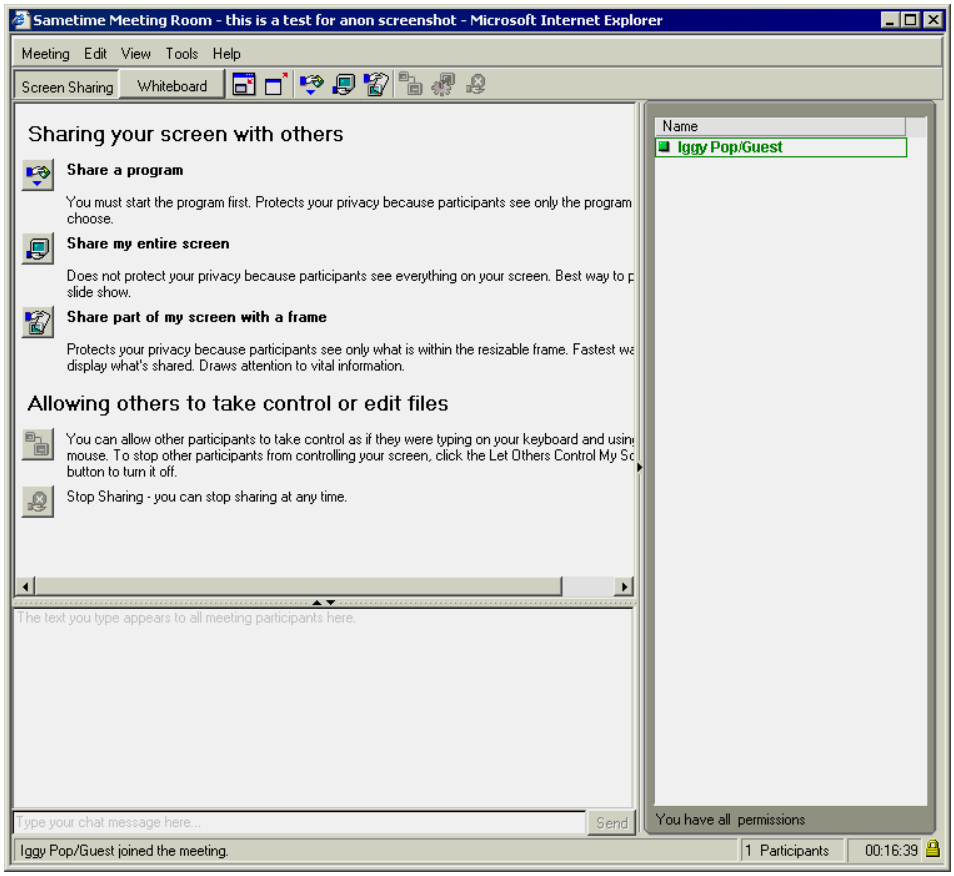


Figure 2. Is this person really Al Zollar

1.1.2 Integrating Sametime 2.0 into an existing Domino domain

This method of installing Sametime 2.0 doesn't provide any real benefits above and beyond installing it on top of an existing Domino server, described previously. However, there are some additional pre-installation tasks and potential pitfalls associated with this installation method.

1.1.2.1 Why install Sametime 2.0 in this manner

Under this method of installation, Sametime 2.0 will take up less disk space and you are able to use your organization's existing Domino Directory.

Larger sites should note that the Domino Directory will be replicated during the installation from an existing Domino server in your organization.

1.1.2.2 Pre-installation checklist

Be sure to complete these mandatory pre-installation steps. Refer to the installreadme.txt file shipped with the Sametime 2.0 Beta 2 distribution, prior to beginning installation, for additional steps and background information.

- If you are installing Sametime 2.0 on Windows NT or Windows 2000, make sure that you disable Internet Information Server (IIS). Make sure that the service will not start on a subsequent reboot. If IIS is running, Domino will be unable to start the HTTP task. The HTTP task must be running under Domino for Sametime to function.
- You must have a working Domino server with a minimum release level of 5.0.3 that contains your production Domino directory. Sametime 2.0 will replicate the Domino Directory from this server to your Sametime server during the installation process.
- Sametime uses agents that must access the Domino Directory. The minimal access level required for these agents is reader. Therefore, you should set the default ACL entry for the Domino Directory to Reader.
- If it is your organization's policy to maintain a No Access setting for the default entry of the Domino Directory, you must add the "Sametime Development/Lotus Notes Companion Products" ID to the ACL with a minimum access of Reader.
- Ensure that all applications on the target PC are shut down.
- If you will administer the Sametime Server via Internet Explorer, you must switch off HTTP 1.1. The administration client will not function correctly if HTTP 1.1 is enabled. Refer to 1.2.4, "Disabling HTTP 1.1 support in Internet Explorer" . Netscape users will not have this problem: by default Netscape uses HTTP 1.0.

1.1.2.3 Directory considerations

The directory considerations for this method are the same as those for installing on top of an existing Domino system, described in 1.1.1.3, "Directory considerations" .

1.1.2.4 Potential pitfalls

The installation will fail if it cannot contact the Domino server that you are replicating the Domino Directory from. If this happens, you don't need to back out of the installation entirely. After you have rectified the problem on the target Sametime machine you can resume the install by running `stsetup.exe` which is located in x:\sametime.

Administrators should note that the default ACL setup of the Sametime Meeting center will allow full anonymous access via a Web browser. This

means that any user in your organization that can access the Sametime Server via a Web browser can start and attend meetings under any name they choose. It may not be obvious to new users that this has happened. There are steps you can take to prevent this; see 1.2.2, “Securing the meeting room” .

1.1.3 Web only

The Web only installation of Sametime 2.0 will allow the Sametime server to act as an LDAP client or use the Domino directory to store user credentials.

This is the only method of installing Sametime that will allow you to take advantage of LDAP support.

1.1.3.1 Why install Sametime 2.0 in this manner

There are two main reasons to use this method of installation: if your organization does not have an existing Domino infrastructure or if you already have an existing LDAP directory.

1.1.3.2 Pre-installation checklist

- If you are installing Sametime 2.0 on Windows NT or Windows 2000, make sure that you disable Internet Information Server (IIS). Make sure that the service will not start on a subsequent reboot. Domino will be unable to start the HTTP taskif IIS is running. The HTTP task must be running under Domino for Sametime to function.
- The installation program will prompt you to choose a directory type: either Domino directory or LDAP directory.
- If you chose LDAP directory you will need the following information:
  a. DNS name or IP address of the server containing the LDAP directory.
  b. The IP port number the LDAP server listens for requests on, usually 389.
  c. The full distinguished name and password of a directory entry on the LDAP server. Sametime will require read access.
- Ensure that all applications on the target PC are shut down.
- If you will administer the Sametime Server via Internet Explorer, you must switch off HTTP 1.1. The administration client will not function correctly if HTTP 1.1 is enabled. Refer to 1.2.4, “Disabling HTTP 1.1 support in Internet Explorer” . Netscape users will not have this problem: by default Netscape uses HTTP 1.0.

1.1.3.3 Directory considerations

The choice must be made between using LDAP and the Domino directory.

By default, the Domino Directory will be used. This means that each user will require an Internet name and password in their person record.

There are two ways to add users when using the Domino directory. Users can be entered into the Directory via the Sametime administration client or via self registration.

Online documentation on adding users via the Sametime Administration tool can be found in the Sametime Administrators guide(sthelpad.nsf) in the section entitled “Adding users from the Sametime Administration Tool (Web-Only)”.

Self registration is not set up by default. If you are using self registration, be aware that anonymous Web users can register any username and Internet password combination. The implication of this is that someone may register under the company CEO’s name or impersonate another person in your organization. For instructions on how to set up self registration refer to the “Enable self registration in the Sametime Administration Tool” section in the “Using Domino Directories with Sametime” chapter in the online Sametime Administrators Guide.

1.2 Installation tips and tricks

This section contains some tips and tricks we gathered when installing Sametime ourselves. Following these hints will make for smoother deployments for you, as it did for us.

1.2.1 Multi-server Sametime installations

1.2.1.1 Standard names

It really helps to have some standard names and IDs in place when you will deploy more than a few servers. Since each server must be made aware of the others in its community, its much easier to verify your connections if the names follow a convention of some kind.

For example, you may name your Sametime servers in the manner shown in Table 1.

Table 1. Examples of standard Sametime server names

Standard Name	Meaning
apacst01.fishnet.com	Asia/Pacific (APAC) sametime server, serving users in the Asia/Pacific region
emeast01.fishnet.com	Europe/Middle East/Africa (EMEA) sametime server, serving users in the EMEA region.
latamst01.fishnet.com	Latin America (LATAM) sametime server, serving users in the America's

1.2.1.2 DNS entries

Make sure you have all your server names registered in your organization's Domain Name Server (DNS). Every Sametime meeting must be accessed via a fully qualified server name that resolves to an IP address. If you access a meeting via an IP address, the Sametime meeting room client will not function.

1.2.1.3 Load balancing

At this time there is no dynamic load balancing system. You can assign each user to a specific Sametime server as their 'home' server. This is where their user buddy list and privacy settings are stored. This is the Lotus preferred method of operation. However, if this server goes down, your users will not have access to any Sametime services, even though other servers could be available for a connection.

You can achieve a form of automated load balancing by using a round-robin or some other form of DNS distribution method, and assign a user to any available server for community services. This gives some recovery if a server is unavailable. Users simply log off and back on again.

But in doing this, Sametime users will not have a 'home' server, and thus the server-stored user list and privacy file will not be usable.

We feel that much more work on automatic load balancing and fail-over needs to be done before we can recommend using anything but the Lotus method.

1.2.1.4 Server network distribution

There are several options that can help you make your networking and server placement more efficient. These are described in detail in 2.4, "Servers" .

1.2.1.5 Large directory system options

This is discussed in detail in 2.7, “Directory services” .

1.2.2 Securing the meeting room

Securing the meeting room will prevent anonymous users from creating and attending meetings. You can also fine tune the actions individual users or groups of users can perform on the Samtime server. For example, you may wish to allow all users in your organization to attend meetings, but only allow a certain set of users to schedule meetings.

Security is implemented using standard Domino ACLs. For details on all of the security options available, refer to the “Managing Security” chapter in the Sametime 2.0 Administrators Guide.

Security can be managed from the Sametime Administration Client or a Notes Administration client.

To force users to authenticate when entering the meeting room, you should set the Anonymous entry to “No Access” in the ACL of the stconf.nsf database. Once Anonymous is set to “No Access,” all users who authenticate will receive the privileges associated with the Default entry.

The following steps outline how to set the Anonymous entry to “No Access” by using the Sametime 2.0 Administration Client. This can also be performed via a Notes client as well. You will need to be signed on as the Sametime Administrator in either case.

1. Start the administration client by clicking the “Administer the Server” link from the Sametime 2.0 default homepage. The administration client will launch in a separate browser window.
2. You should see the Server overview as shown in Figure 3 on page 11.

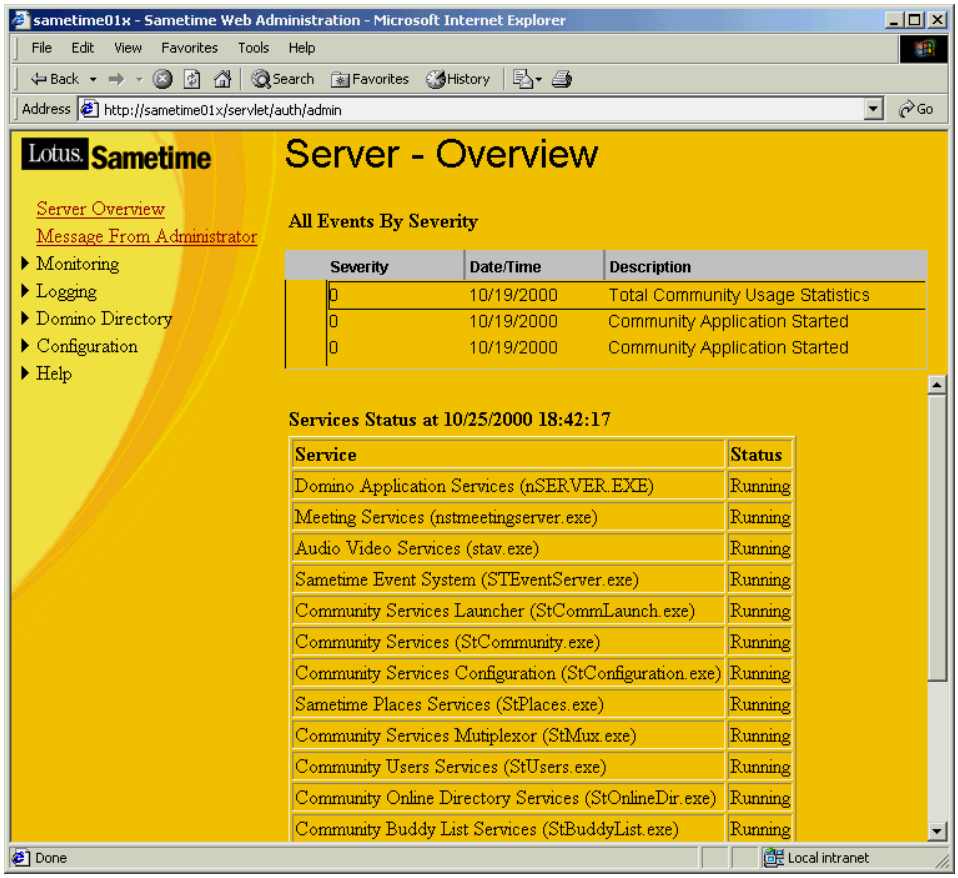


Figure 3. Initial screen in Sametime administration client

3. If you are using an LDAP directory to store user information, expand the LDAP Directory Link; if you are using a Domino directory, expand the Domino Directory Link.
4. Click on the Access Control link. You should now be at the Access Control screen shown in Figure 4 on page 12.

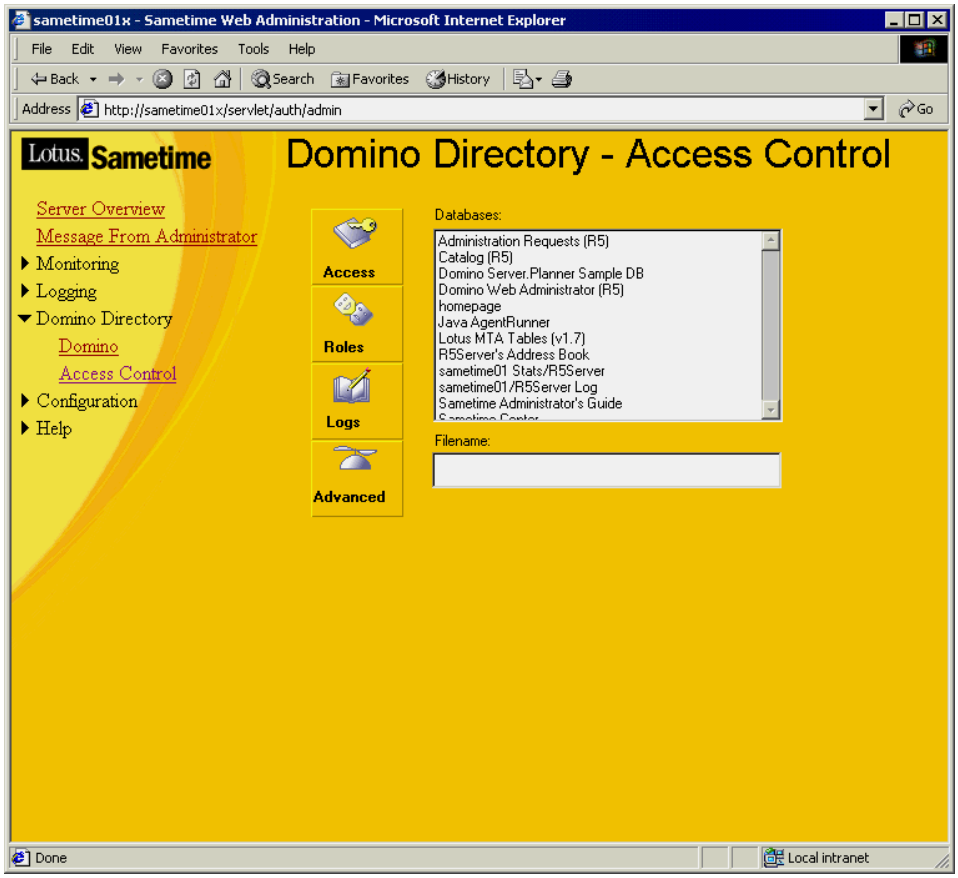


Figure 4. Database access control screen in the Sametime administration client

5. Enter `stconf.nsf` into the Filename text box and click the Access button. The stconf.nsf database contains the forms used to schedule meetings and generates the links users follow to attend meetings. Your screen should now look like Figure 5 on page 13.

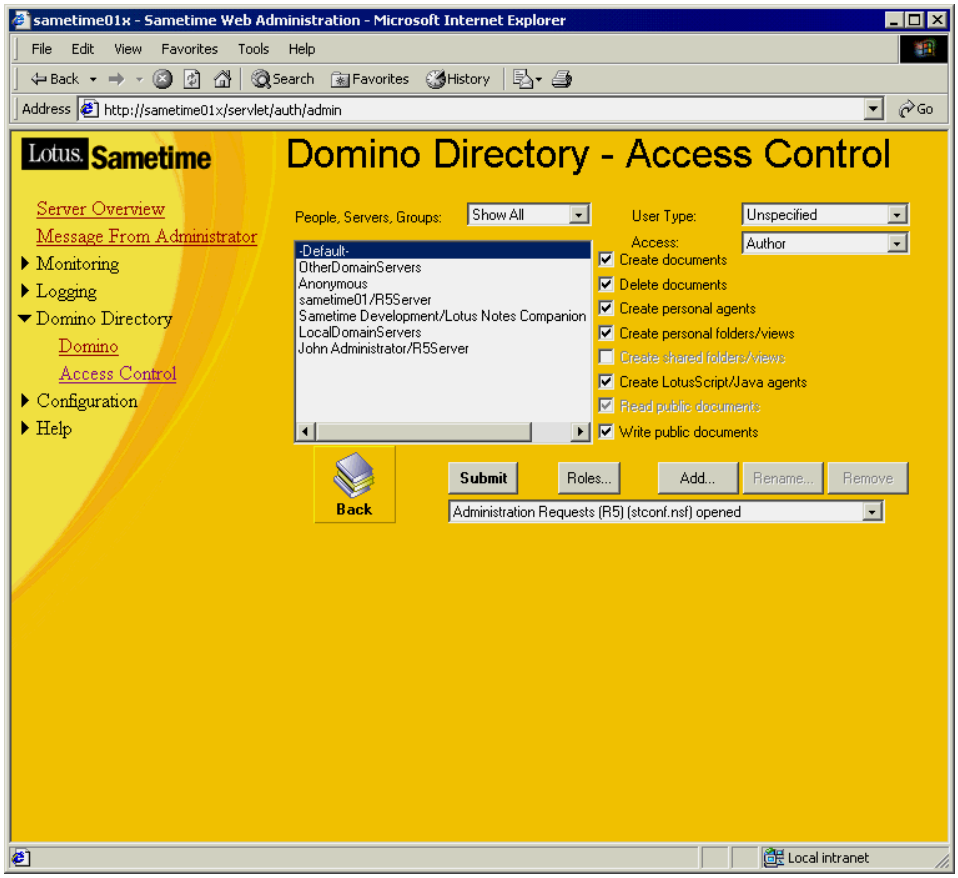


Figure 5. Database ACL in the Sametime administration client

6. Click on the Anonymous entry in the People, Servers, Groups selection list
7. In the Access section select No Access.
8. Deselect Read public documents and Write public documents.

9. The ACL setting for Anonymous should now look the same as Figure 6.

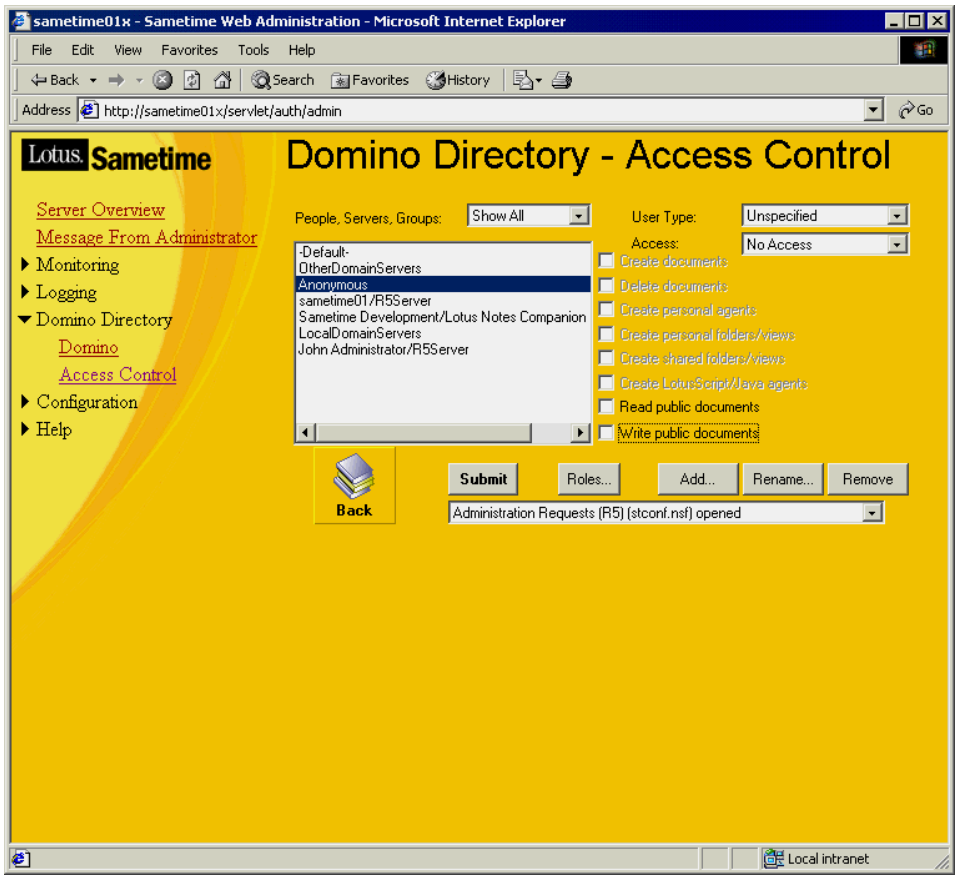


Figure 6. ACL settings to prevent anonymous access in the Sametime administration client

10. You must click the Submit button to apply the changes.

If you would like more granular control over the actions of groups of users or individuals, you can configure the ACL so that some users can only attend meetings and other users can attend and create meetings.

To allow a specific group of users to create meetings you should create a group with access of “Author” and give them the “Write public documents” privilege.

Users that can only attend meetings should be given an access level of “Reader.”

1.2.3 Customizing the Sametime homepage

You can customize the links that appear on the homepage via parameters in the notes.ini file. Using ini parameters to remove the links from the homepage does not make these areas secure, since they can still be accessed by the full URL.

Important

These INI parameters are an undocumented feature of Sametime 2.0; therefore, they are unsupported.

Set the corresponding parameter to 0 for the link you would like to remove. That is, if you would like to remove the link to the administration client, make the following setting in your notes.ini:

```
$STServerAdminInstalled=0
```

Table 2 provides a description of the parameters and the links they allow you to customize.

Table 2. Sametime homepage NOTES.INI parameters

INI Parameter	What does it do?
$STMeetingCenterInstalled	Controls the display of the “Attend a Meeting” and “Schedule a Meeting” links on the homepage
$STDiscussionsInstalled	Controls the display of the “Use Discussions and Teamrooms” link
$STClientPackageInstalled	Controls the display of the “Download Sametime Connect” link
$STQuickStartGuideInstalled	Controls the display of the “Quick Start Guide” link
$STDocumentationInstalled	Controls the display of the “Documentation” link
$STServerAdminInstalled	Controls the display of the “Administer the Server” link, which is located in the page footer

The notes.ini variables described in Table 3 will be in the first customer shipment of Sametime 2.0. They were unavailable in Sametime 2.0 Beta 2 and were therefore not tested as part of this redbook project.

Table 3. Untested Sametime Homepage NOTES.INI parameters

INI Parameter	What does it do?
$STToolkitInstalled	Controls the display of the toolkit link
$STDevForumEnabled	Controls the display of the “Developer Forum” link
$STLotusLinkEnabled	Controls the display of the “Lotus” link, which is located in the page footer
$STIbmLinkEnabled	Controls the display of the “IBM” link, which is located in the page footer
$STDisplayLogins	Controls the display of the login link

1.2.4 Disabling HTTP 1.1 support in Internet Explorer

Accessing the Sametime Administration client with an HTTP 1.1 browser is not supported. Perform the following steps to disable HTTP 1.1 support in Internet Explorer. Netscape supports HTTP 1.0 and will work without any extra configuration.

Note that users will not need to perform these steps in order to use Internet Explorer to attend Sametime meetings.

1. Launch Internet Explorer.
2. Select **Tools -> Internet Options** from the menu bar.

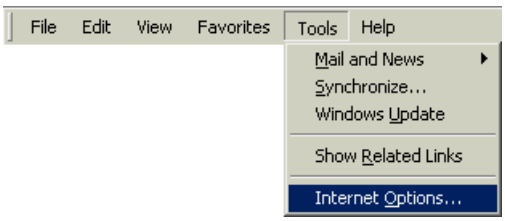


Figure 7. Selecting Internet Options in Internet Explorer

3. Select the Advanced tab from the resulting dialog box.
4. Scroll down until you see “HTTP 1.1 Settings” and deselect “Use HTTP 1.1” (see Figure 8 on page 17). Click OK.

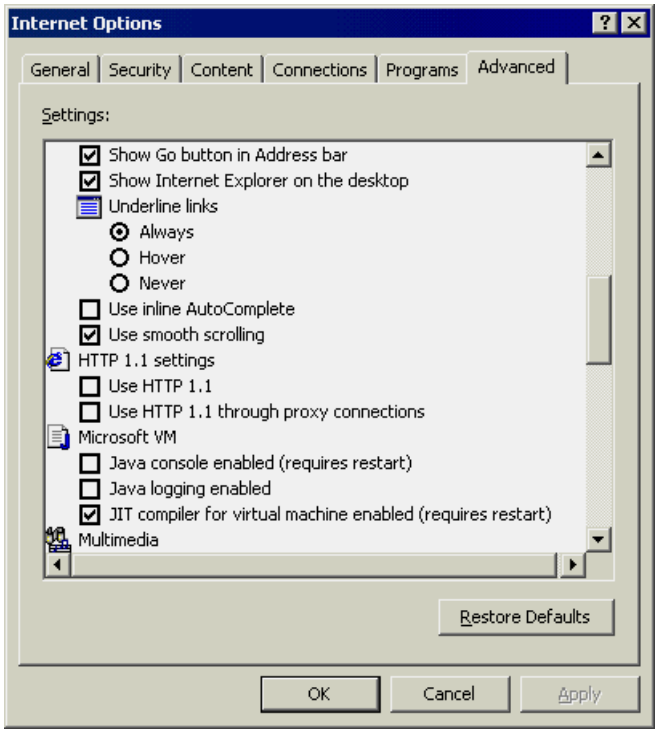


Figure 8. Disabling HTTP 1.1 Support in Internet Explorer

You have now successfully disabled HTTP 1.1 support in Internet Explorer.

1.3 Client download and installation

A successful distribution strategy for the Sametime Connect client is an integral part of a successful deployment. This section outlines various ways the distribution can be achieved and presents some caveats regarding end user workstation configuration.

The full Sametime Connect client is 4.7 MB in size, but it can be pared down considerably if you choose not to package some options.

Use the Sametime Client Packager to customize Sametime for your deployment and to simplify the installation process for the end users. Details about the Sametime Client Packager are in 1.4, “Sametime client packager” .

1.3.1 Options for distributing the Connect client

We have considered four options for distributing the Connect client out to existing end users. These options are discussed below. This section applies to Windows OS systems only.

1.3.1.1 Download from Sametime 2.0 server

Downloading the Sametime Connect client from the Sametime server homepage is by far the simplest option. It requires no setup since it is a part of the default Sametime 2.0 installation.

This option is very easy for end users to perform because the website provides on-screen instructions that detail what the Client Package is and the name of the user's Sametime Server.

However, if this option is used, the server will be unnecessarily loaded during the early stages of the deployment as large numbers of end users download the client package. End users will also have to specify their home Sametime Server during the install.

This option works well for smaller Sametime deployments with one server, in sites that have no set distribution method for software, or in organizations that have the server resource to handle the initial rush to download.

1.3.1.2 FTP

Posting the packaged client on any accessible FTP server is another way to make the client available to your organization.

Client FTP is relatively simple to set up and administer. If Windows 95 or above is being used as the operating system on the corporate desktop, all of your users will already have a command line FTP client installed on their machines.

However, the command line FTP client is very terse, and often results in problems as users unfamiliar with it are required to make the distinction between ASCII and binary files when downloading.

The use of a graphical FTP client such as CuteFTP or FTP Voyager may help to simplify the process a little bit, but this is yet another piece of software that your users must configure.

The easiest way to access an FTP server is via your standard Web browser, using ftp:// instead of http:// to reach the designated FTP server.

FTP is a good fit for most deployments where the majority of users are familiar with the use of FTP or already have working GUI FTP clients.

1.3.1.3 User distribution systems

The Sametime Connect client comes as a single InstallShield install package, following all the install conventions of any other standard application package made for Windows.

Using your choice of methods (Website link, CD-ROM, shared file, E-mail attachment) you can distribute this file for all users to store and execute on their local PC. If you include the INI file, the install options for end users will be restricted to selecting the directory to install Sametime Connect and clicking on the “Next” button a few times. Refer to 1.4, “Sametime client packager” for details.

1.3.1.4 Automatic file update systems

There are numerous “push” software distribution systems that load new software onto users’ PCs from a central server via a script or automated toolset. Any system you use can be put to work for distributing Sametime Connect.

Since there are no special tricks during Sametime code install, your standard install scripts and packaging tools should be sufficient. However, you should notify new users by other methods that this program is to be installed, and what their ID/password is to be.

If you are using a Domino or LDAP directory service for IDs, you should also make sure the fields for the Sametime home server, ID, and password are populated before distribution begins.

No matter what method you use, it’s always helpful to point out where the help is if users have trouble. And be sure to educate your support staff about what you are doing — they usually hate surprises.

1.4 Sametime client packager

The Sametime client packager is used to build customized installation archives of the Sametime Connect Client.

The client packager allows administrators to specify the functionality they would like to include in the Connect client and the default settings for home Sametime servers and proxy servers.

Use of the client packager will result in smoother installations for end users since they no longer have to specify the correct Sametime server or proxy servers.

1.4.1 What can be customized with the Sametime client packager

The following functionality can be removed from an installation of the Connect client.

Table 4. Functions that can be removed from a Connect client distribution

Function	Description	Size
Sametime 1.5 Compatibility for Data Sharing	Supports backward compatibility for screen sharing and shared whiteboard in instant meetings	1191 KB
Directory Browsing	Allows browsing of the corporate directory by the client	292 KB
AOL Instant Messenger Connectivity	Allows users to see when AOL Instant Messenger users are online and send them messages	410 KB
Print Capture Utility	Allows users to create an image they can attach to the Whiteboard by printing from a program	322 KB
Plug-in for Microsoft Netmeeting	Allows users of Netscape to launch Microsoft Netmeeting from the Meeting Centre (in order to join a meeting)	830 KB

The following settings can be given default values:

- Sametime server name and port number
- Screen Sharing port number
- Sametime server proxy
- AOL Instant Messenger server name and port number
- AOL server proxy
- Keep alive time-out interval

It is also possible to provide a customized connect.ini file. This can be useful if you want to provide all of your users with a default set of status messages that are different from the ones supplied with the product.

1.4.2 Potential pitfalls with the Sametime client packager

If a connect.ini file is not specified during the configuration of a client package, the community port setting will be incorrect in the resultant install.

The community port is set to 8081 instead of 1533, even though 1533 is specified by default in the client packager. This will cause the Connect client to wait for a long time since it cannot connect to the server on that port.

This problem can be easily worked around by setting up a connect.ini file and specifying the location of the .ini file during the setup of the client package, as described in the next section.

1.4.3 Modifying connect.ini

The connect.ini configuration file is used to specify proxy settings, Sametime server settings, default status messages and numerous other settings associated with the Sametime client.

Do not create connect.ini from scratch. Perform an installation of Sametime Connect and copy the connect.ini file to another directory. Make any required modifications to the copied file.

The majority of the connect.ini variables and their meanings are self-explanatory. Table 5 outlines some of the main connect.ini variables and what they are for.

Table 5. Selection of connect.ini variables

Variable Name	Meaning
Server Port	Specifies the TCP/IP port setting for Community Services, by default this should be set to 1533.
User	Contains the username used in Sametime
AutoLogin	0 for manual login or 1 for automatic login
AppShare Port	The application sharing port, by default 8081
Server	The name of the server in the following format, server.lotus.com
Messagex	Contain the status messages used in the client. The number is used to specify the position in the dropdown list i.e. Message0 will be the first message in the list.

If you use connect.ini to set up a customized client package, you should set the user variable to blank, that is User= , since this will cause the client to

prompt the user for their name. The AutoLogin variable should also be set to 0. Refer to the sample connect.ini that follows.

```
[Login]
Server=stexternal.fishnet.com
Server Port=8082
AppShare Port=8081
Proxy Type=0
Proxy Host=
Proxy Port=
Socks Type=0
KeepAliveTime=60
Proxy User Name=
Proxy Password=
User=
Password=
AutoLogin=0
AOL ScreenName=
AOL Password=
AOL Autologin=0
ResolveLocaly=0
[Setting]
ShowAddMessage=1
AlwaysOnTop=0
WindowSize=709,48,992,427
StatusBar=0
[Aim Connectivity]
User Name=
Password=
Auto Login=0
Server Host=login.oscar.aol.com
Server Port=5190
Proxy Type=0
Proxy Host=
Proxy Port=1080
Socks Type=0
Proxy User Name=
Proxy Password=
[AudioVideo]
Microphone=0
Speaker=0
Video=0
[StartUpWindows]
ShowMyAvailableToolsDlg=0
ShowAudioVideoWizard=0
ShowAimDlg=1
[ActiveMessages]
```

```
Message0=I am Active
Message1=I am at work
Message2=
Message3=
Message4=
Message5=I am Active
[AwayMessages]
Message0=I am away from my computer now
Message1=I am in a meeting
Message2=
Message3=
Message4=
Message5=I am away from my computer now
[DNDMessages]
Message0=Do not disturb me
Message1=I am busy working
Message2=
Message3=
Message4=
Message5=Do not disturb me
```

1.4.4 Removing AOL Instant Messenger connectivity

This section describes how to produce a client package that does not contain the AOL Instant Messenger connectivity feature. Use the following steps to do this:

1. Run the sametimeclientpackager.exe file.

   The sametimeclientpackager.exe file is located in the x:\SametimeClientPackager directory, where x is your drive letter. This directory will be created when you expand the Sametime 2.0 Beta 2 archive on your machine.

2. The client packager uses the Windows InstallShield to guide you through the setup. Follow the on-screen instructions and click on Next to proceed.

3. The screen shown in Figure 9 on page 24 contains the list of what components can be removed from a given client package. Deselect AOL Instant Messenger compatibility.

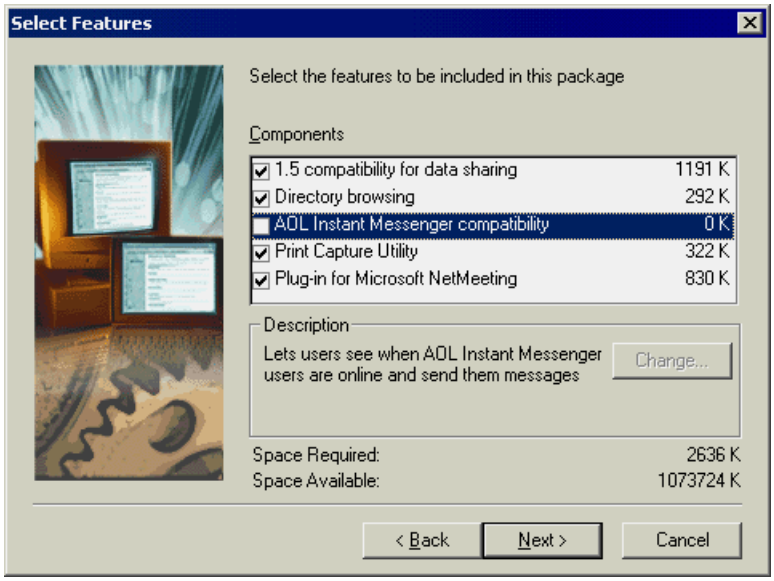


Figure 9. Components that can be removed from a Connect Client installation

4. Optionally, you can specifythe location of a connect.ini file.
5. Specify the Sametime server name and TCP/IP ports it will use for Community Services and Screen Share.
6. Specify the type of proxy you use for Sametime (if any). If you choose a proxy you will be prompted for the proxy server's name and port number in the subsequent screens.
7. Specify a keep alive time-out interval.
8. You should now be presented with a summary of what will be included in your package, as shown in Figure 10 on page 25. Click Next to continue.

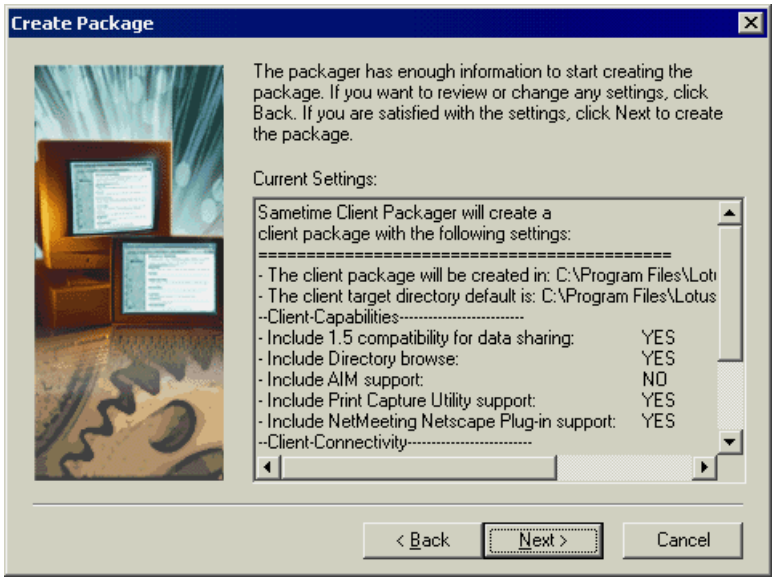


Figure 10. Summary of components included in a client package

9. The client packager will build the client. You should see a progress indicator on the screen.
10. You have now successfully built a client package. It will be located in the directory you specified at the beginning of the wizard. Click Finish to exit the client packager.

1.5 Summary

In this chapter we have discussed the three options for installing Sametime, namely installing Sametime on top of a Domino server, integrating a standalone Sametime server into an existing Domino domain, and a Web-only installation of Sametime. We have provided you with information on the benefits of each method of installation so that you can more easily decide which one you will perform. We have outlined the steps you must take prior to following each of the three installation paths and provided information on some of the pitfalls we found during our testing and how you can avoid them. We have also discussed some tips and tricks that we have found useful in Sametime deployments we have worked on and provided details on options for distributing the Connect client package throughout your organization. Finally, we discussed how to use the Sametime Connect client packager to customize the Connect client and provide an example of how to remove AOL Instant Messenger functionality.

Chapter 2. Planning a Sametime 2.0 deployment

The deployment of any product is always made easier by asking as many questions as possible before starting. The installation of Sametime Connect is not as complicated as that of many other software products, though it still requires good planning for a smooth start. This chapter discusses the issues you should consider before you start installing Sametime.

The major items to consider are: population, clients, servers, networking, Sametime 1.5 upgrades, and the directory service you choose.

We also included a short list of human factors to consider, which may influence the deployment and use of Sametime in your organization, and may provide some food for thought.

2.1 Population

The population questions to consider in a Sametime deployment are:

- How many people in your organization will use Sametime concurrently?
- How many people will use this application overall?

To get into more detail, what types of Sametime services will they be using? What services do you need for your business? Since each Sametime service has a different impact on your networks, servers, and clients, looking first at your user population and their needs will give you a good perspective when working though the remaining questions in this chapter.

There is no “one size fits all” when it comes to planning for Sametime (or any other deployment for that matter). One useful approach is to list all functions of Sametime and then estimate the number of users of these functions at *any given moment in time*. It’s fair to assume that all users will, at some point, use everything that Sametime Connect has available. For most planners, this will be a rough estimate, but it will give you a base from which to work and to anticipate other issues that might come up as you go through this chapter.

For example:

Fishnet Corp has 17,000 employees worldwide, with about 9,000 of them in offices or connected to the network on a more or less constant basis. Of those 9,000, there are two groups of technical support personnel that need to stay in constant contact with each other, and two groups of sales teams that are heavy users of online presentations to management and external

customers. Therefore, your estimates of Sametime usage at Fishnet Corp might look like Table 6.

Table 6. Estimates of FishNet's Sametime functions and peak concurrent users

FishNet Corp	Text IM	Online Meeting	A/V Broadcast	2-way Audio only	2-way Audio Video
Sales Dept	6000	50	100	250	10
Tech Support	500	10	1	10	5
Executive	100	20	<1	1	5
Admin	2000	1	<1	<1	<1

However you plan your capacity, make sure you leave a lot of flexibility for surges in demand—like a CEO broadcast to all employees, or a sudden jump in audio conference calls as new audio-equipped PCs are deployed in a department.

2.2 Client PC

The client PC provides all of the power required to send and receive Sametime awareness data, instant messages, audio, and video services. All audio and video codec processing is performed on the client PCs. The Sametime servers do not do any manipulation of the contents of data packets sent through them.

The local PC also downloads (from a Sametime server) and executes the signed Java applets used in meetings and for providing the audio/video interface.

Given these functions, the client PC must have sufficient power to support demands placed on it by Sametime. Almost any currently used Windows 95 PC with a network connection will be able to handle text IM, and the object sharing/whiteboard sessions (slow PCs will take a considerable length of time to start Java applets though). The demands on the client PC rise sharply when audio and video compression and handling for these functions are introduced into the picture.

Table 7 on page 29 shows what impact each Sametime service can have on the overall capacity of a single server. Note that any increase in one service can reduce the amount of server capacity for other Sametime services.

If you have a single Windows 2000 Server, running on a 500MHz PentiumIII dual processor with 1GB of RAM and 10 GB of disk, you could expect to be able to support one of the functions listed in the table at any given time.

Table 7. Capacity of a single server for each Sametime function

Sametime function	Maximum users
Community Services/Text IM	10,000 (all online with Connect client)
Application Sharing/Whiteboard	500 (10 meetings of 50 users each)
A/V Broadcast meeting	300 users watching (need confirmation)
A/V Broadcast meeting via IP Multicast	Unlimited users watching*
2-way audio conference	200 (100 meetings of 2 users)
2-way audio/video conference	100 (25 meetings if 4 users)
Full interactive meeting with audio/video	100 (10 meeting of 10 users)

* Assumes that network is fully IP Multicast enabled. Users unable to use multicasting will connect directly with broadcasting server.

As you can see from this table, a large number of concurrent users for anything but text IM significantly raises the number of servers required in total, or greatly reduces a single server's capacity to support other functions. A system administrator can set the limits for each function to prevent one function from overwhelming the server.

Remember that an increase in the use of one service will reduce the capacity in another service area. If you have 5000 community users online already, the other functions will have that much less resource to use.

Given the wide variety of hardware in use, it's difficult to estimate the exact capacities of any one server. One way to conceptualize this is to imagine that a server has a total number of "points" available, and each individual service uses a particular number of those points. Roughly 1 point per community connection, 10 points per meeting, and 20-30 points per audio and video transmission might be used, and decremented from the total points available on the server.

2.3 Client networking

Every Sametime service is only as good as its connection to the users. When planning your Sametime deployment, keep you users' networking capacity in mind. Consider questions such as: Are you using low-bandwidth connections

from remote sites? Are all your users in one site, or are they scattered across the world? How congested is your current network?

Sametime does not use the peer-to-peer network model that some other conference tools do (like Microsoft's NetMeeting), so all communications *must* be routed through a Sametime server. The advantages of this become apparent once you move beyond small meetings and into larger interactive meetings or the broadcast service.

Table 8 gives a rough outline of what Sametime functions are acceptable at each network connection speed. Keep in mind that every network is different, and issues such as network traffic congestion and line speed fluctuations are not considered here.

Table 8. Recommended bandwidth and performance levels for Sametime functions

Line Speed (Kbps)	**Text IM <1 Kbps**	**Broadcast Meeting 16-128 Kbps**	**AppShare/ Whiteboard 3-64Kpbs**	**2-way Audio 6.3 or 64 Kbps**	**2-way A/V 16-128 Kbps**
<56K	Good	Audio OK, video not recommended	View OK, pre-load files for presenter*	OK - listen only broadcast	Slow 1 fps
56K-64K	Good	Acceptable	Live screen share OK in limited size, low colors	OK if used with moderated microphone	Marginal
128K-300K	Good	Good	Good	Good	Reasonable
>300K	Good	Good	Good	Good	Good

* Pre-loading files gives slow connection users a performance boost as the previous, current, and next pages of a presentation are cached on local PCs in the background as the meeting progresses.

Note that even very low-speed (28.8 Kbps or lower) connections will function very well for online status and text IM functions. Instant message data transmissions are usually measured in mere bytes (far less than 1K per message), and any lag encountered usually occurs because of routing delays rather than the time required to actually transmit the data.

There are some additional performance tips posted at `http://www.lotus.com/sametime` under Tips and Techniques.

Our experience to date has shown that text IM is the single most popular function of Sametime, and the lightest one in terms of impact on your

network. Therefore, you should have no reluctance implementing IM clients at the end of even the slowest network connection.

Note

If you have network users that are charged by the hour for network time (such as dial-in users), staying online with the IM function can have a sudden impact on your networking costs, since Sametime sends regular traffic over the net to maintain the community status on your network. Sametime will keep your connection alive all the time and defeat any disconnect timers.

2.4 Servers

Sametime servers provide all the traffic control, packet duplication, and meeting management services. The server manages the community connection for each user, serves as the hub for all meeting requests, and maintains order and security for the Sametime clients and meetings.

2.4.1 Single Sametime server

While it is possible to install Sametime on top of other Domino servers (such as a mail or application server already installed), we do not recommend this practice except in a very small organization.

A single dedicated server set up with Sametime can provide sufficient capacity for many operations to get a start with Sametime.

The primary limitation for a single Sametime server's capacity is the number of IP ports that can be maintained by the OS itself. We have estimates of upward of 14,000 on Windows 2000 Server.

For planning, a good rule of thumb is 10,000 users per server for basic community services (awareness and text IM). Fine tuning of Windows server settings, along with high performance network interfaces, may help you get closer to the high end estimates.

Figure 11 is a model of basic Sametime access, with all functions being accessed by clients directly on a single server. Each client PC accesses the Sametime server via the 'mux' (multiplexer) for community awareness on the Sametime server. Meeting users (audio/video/data) are directly connected to the Sametime meeting server functions. Anyone receiving only the

'broadcast' (1-way outgoing) meeting session is connected to the broadcast gateway (BG).

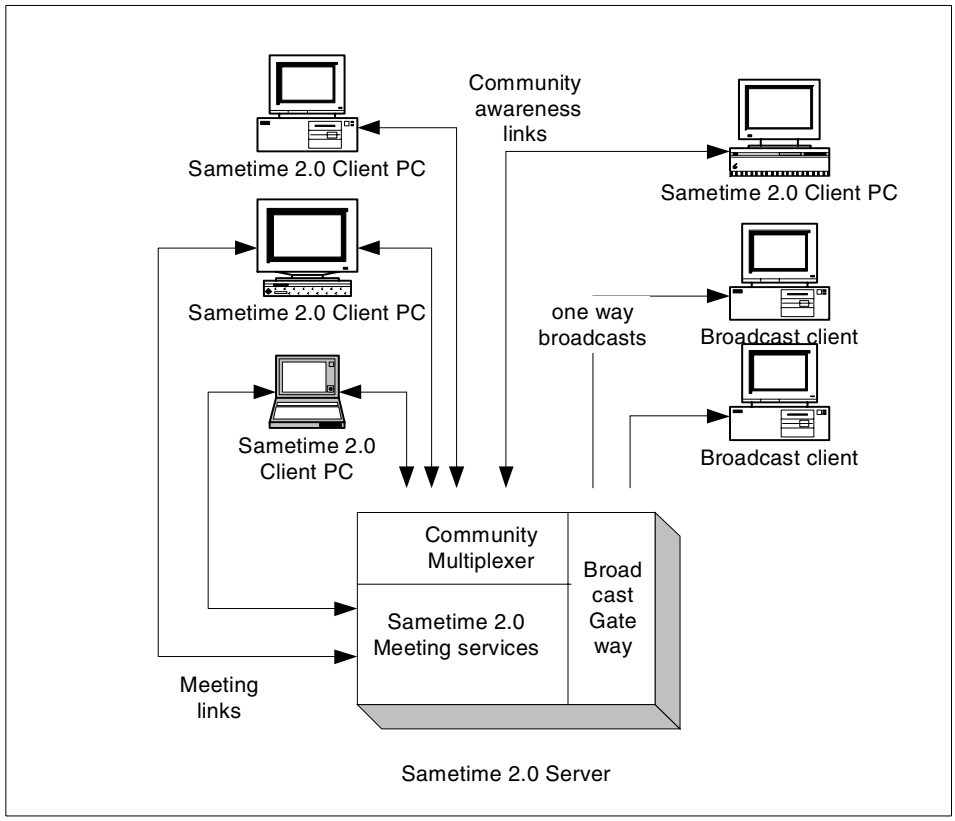


Figure 11. Basic Sametime direct client to server access. Note that we are ignoring all intermediate network steps that may be taken to reach the server.

Take note that in this basic setup, all IP access is established directly with the Sametime server. For small numbers of users (in the hundreds) this may be all you need to set up to get a workable Sametime solution.

Server note

Generally, you will gain more improvement in Sametime performance by having a good network design, and/or more server RAM, rather than having faster or more CPUs.

2.4.2 Multiple Sametime servers

Sametime does not limit you to using a single server. You can establish a large number of servers working within the “community,” providing a single interface to the users, while each server is providing a discreet Sametime service inside.

There are no defined upper limits on how many Sametime servers you can have linked together, but there are practical limits imposed by your network design and server locations.

Sametime services can be split between 2 different types of servers: the community server and the meeting server.

Sametime also allows you to configure servers to provide only designated functions. This allows you to run dedicated community and instant messaging servers, object sharing/meeting servers and/or multimedia servers running within a single address (from the user’s viewpoint) or community connection.

Creating multiple servers allows you to adapt your server setup to meet the increased demand for one function without requiring server overkill in another less used function.

The next two figures show two possible ways you can deploy multiple Sametime servers to take advantage of your network layout.

Figure 12 on page 34 has two Sametime servers located together on the same network segment, configured to be aware of each other. Users connect to one server, obtain the services required, and then the servers relay any information needed to users logged onto the other server that may need to be connected to a chat or a meeting over the server to server linkage.

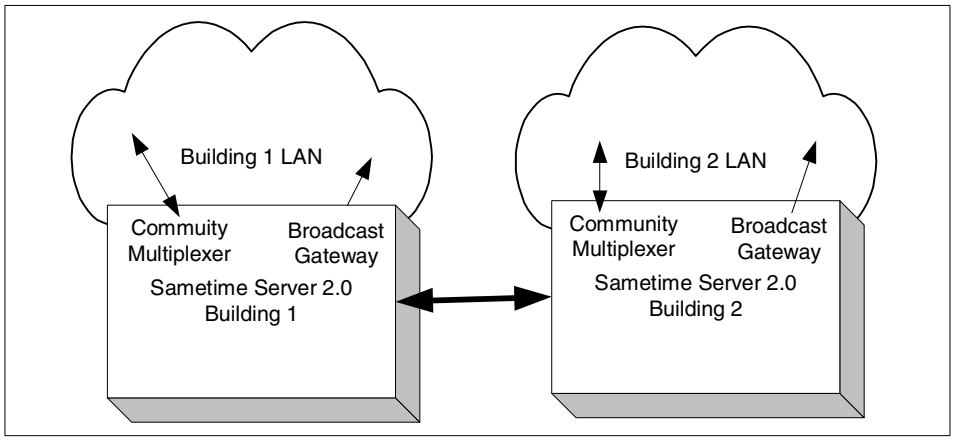


Figure 12. 2 Sametime servers on same LAN segment, each one serving a different building.

You can also deploy the servers over opposite sides of a WAN (between New York and Tokyo for example), to allow them to provide service to their local community and meeting services with minimal delay, and still remain connected to each other over the WAN. This is illustrated in Figure 13 on page 35. The users appear to each other under the same community, despite their physical separation.

Positioning the Sametime servers this way will have the additional benefits of providing local server access for each city and condensing any required traffic between cities over fewer IP connections.

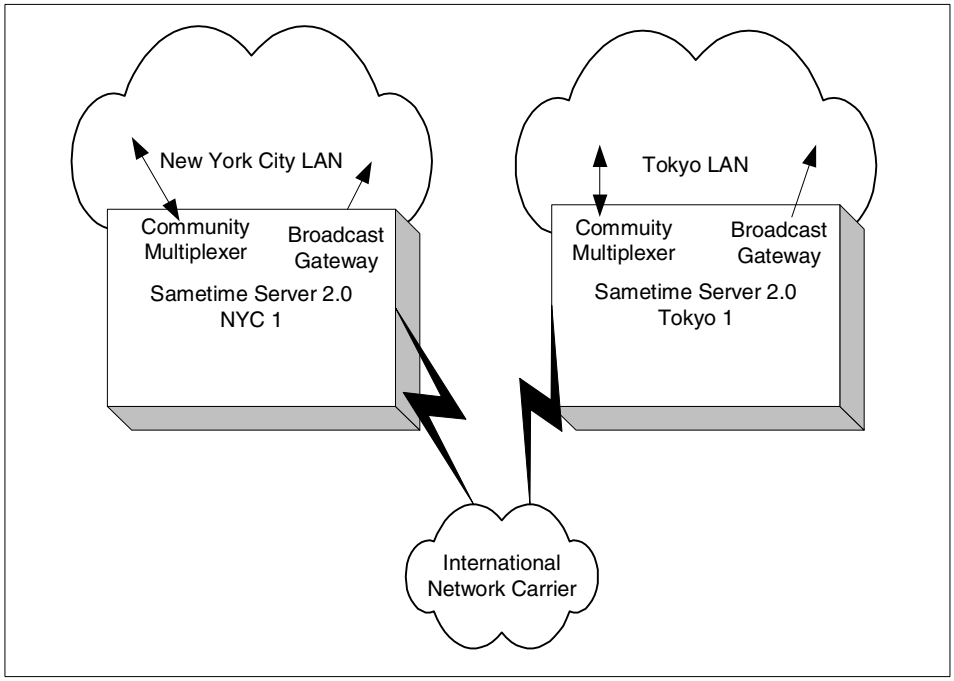


Figure 13. 2 Sametime servers at remote sites, linked via a WAN connection

As you get into larger Sametime deployments, the options and setup naturally grow more complex, but by keeping the essentials in mind, you should be able to design a system that will fit your network's strengths.

Note

There is no "one" recommended way to establish your Sametime services. Each installation will have to also consider unique factors and IT costs before implementation.

2.4.3 Remote multiple Sametime servers

Given the setup in the previous section, you can continue the pattern and establish servers for each logical area of your business, and then link all those servers together.

Figure 14 on page 36 illustrates a case where we have 3 sites to link together.

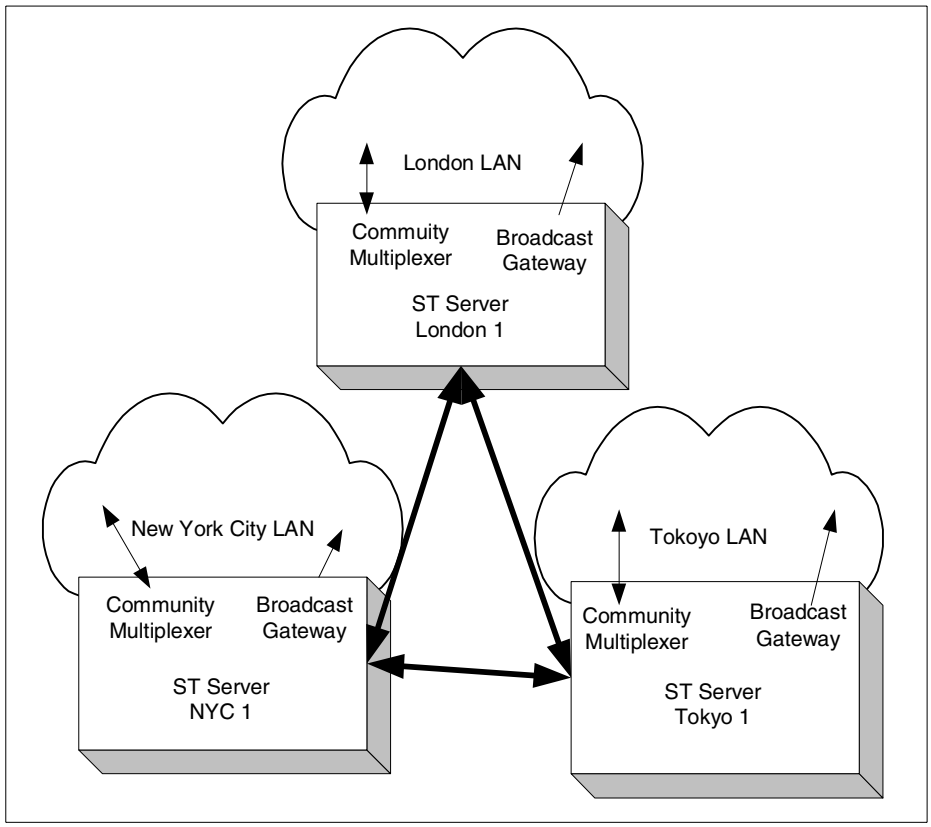


Figure 14. 3 Sametime servers in remote offices connected over a WAN

Each of these three sites operates a local Sametime server; they are linked together via a WAN. Each server provides Sametime community and meeting services for the local population, and relays any required connections or meeting data over the WAN to remote users. Should a WAN link be broken, local services would not be affected. Any remote meeting attendees or chat sessions would, of course, be lost until the links are re-established.

Note

There is no “pass-through” function in Sametime to work around lost connections or a downed server. Sametime will take advantage of any alternate WAN services that you may have in your network by trying to automatically re-establish lost connections.

2.4.4 Option: Separated community multiplexing

One deployment option to consider is not part of a standard Sametime server setup, but is a documented feature called *separated multiplexing*. Normally, each Sametime server contains within itself a multiplexing control system to maintain the active IP ports for community connections to the client PCs.

You can move this multiplexer function to a specialized server and run this function to do nothing but provide the live connections to the clients on one side, and funnel the data down to Sametime via a single IP connection to the server.

Note

Any reference to multiplexers refers only to 'community' services of awareness and text chat. Other services such as whiteboard/app share, audio and video all directly connect back to the Sametime server that is hosting the meeting.

Figure 15 on page 38 shows a circumstance where we have a large number of clients in two separate offices connected to one Sametime server. The muxes provide an expansion of the total number of ports that are available for use, while freeing the actual server from the job of managing most of them. We have one PC acting as a meeting presenter, which directly connects to the Sametime meeting server, and several users that are attending the meeting with the broadcast client software.

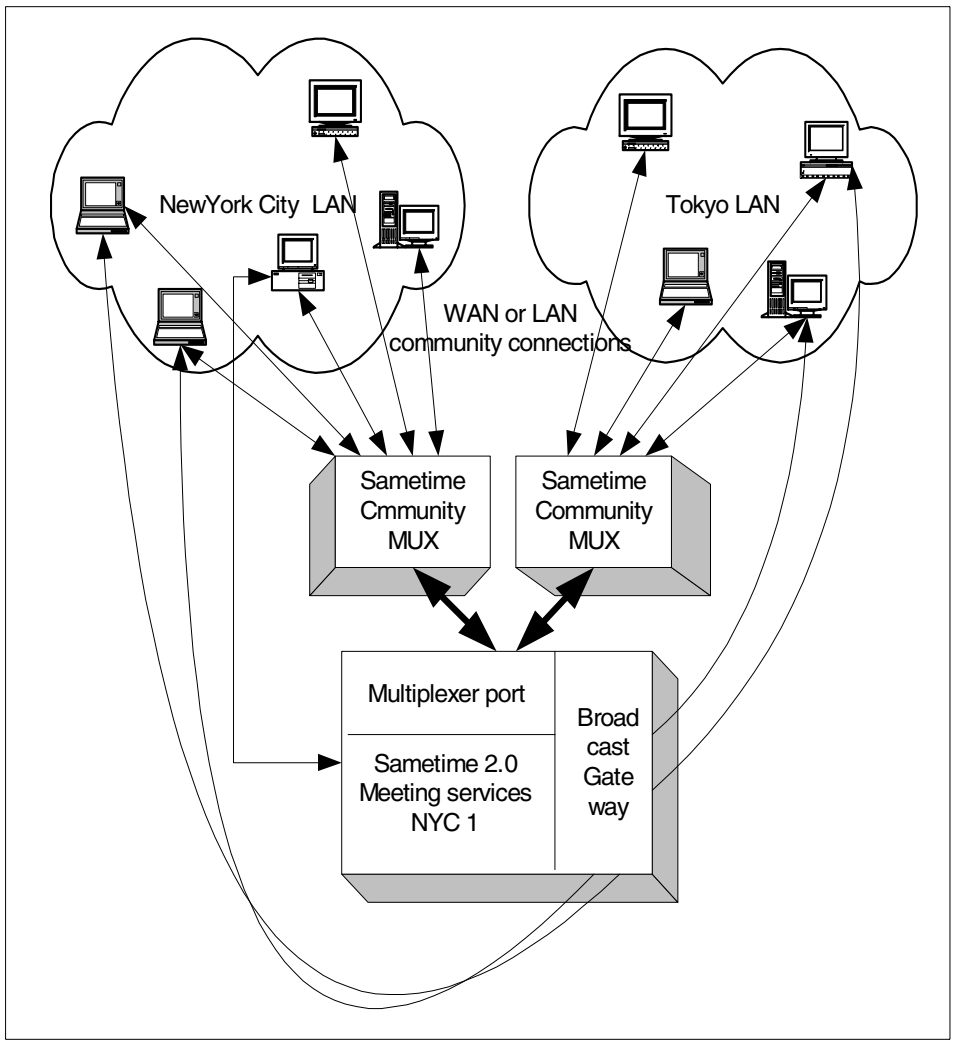


Figure 15. Sametime with 2 multiplexers set up in front of a single server. Note that the meeting and "broadcast" gateway for data,audio, and video streams does not use multiplexers.

Establishing separate multiplexers for Sametime has several benefits for large communities.

It removes the job of managing each individual community connection made during the workday by clients from the main servers. With no other functions running on a multiplexing server, higher levels of stability can be achieved, and networking connections to the servers behind them are optimized.

You can use smaller, less expensive servers for this function since they work only to provide the IP connection services.

You can overcome some of the network limitations of your OS. A single Sametime core server should be able to service upwards of 100,000 active community connections. However, Windows NT and 2000 Server fall far short of being able to support that many IP connections on a single server. A safe estimate is around 10,000 live IP port connections per server. Thus you could install as many as 10 multiplexing servers in front of a single Sametime server.

Figure 16 shows how you can use multiplexing to reduce the port connection load on the actual Sametime server, yet expand the number of connection ports available for users, all without having to add another full server. This works for community services, but interactive meetings or broadcast meetings will still go back to the hosting server directly for their port connections.

This figure shows a series of multiplexers in front of a single server, providing IP ports and reducing the load on the actual server's IP management tasks, and freeing the main server's memory and CPU for providing meeting services.

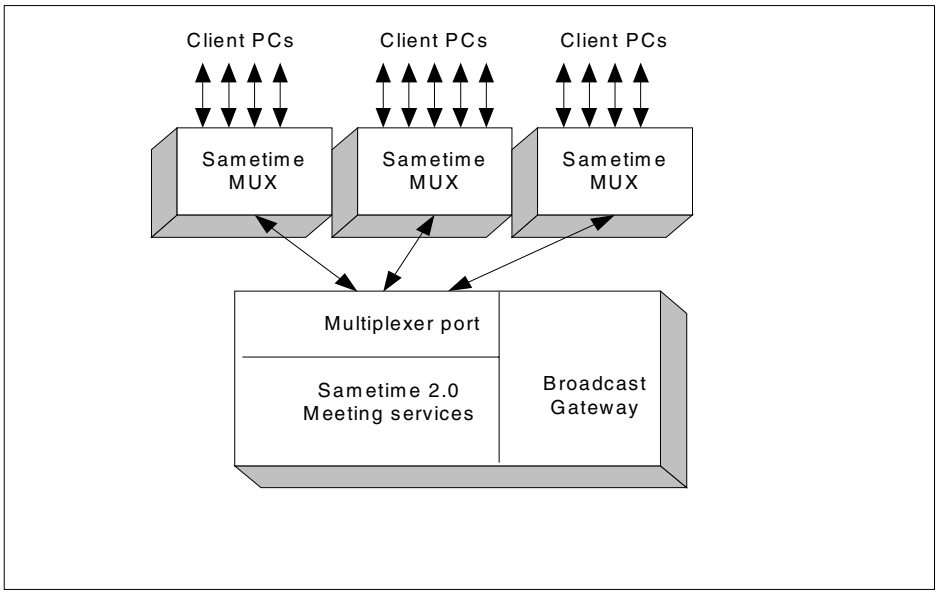


Figure 16. Multiple mux's to reduce IP port connections on Sametime server

Note

Sametime multiplexing services are transparent to the client PC. They simply provide the active port for a client to connect to, and then channel the data down a single IP port to the server. The servers still perform all community and meeting services. If a server goes offline, the multiplexers can do nothing on their own.

Figure 17 illustrates the multiplexers moved to the other end of the network, away from the server location, to reduce WAN traffic. Doing this allows the remote mux to use a single IP port connection over the WAN back to the Sametime server.

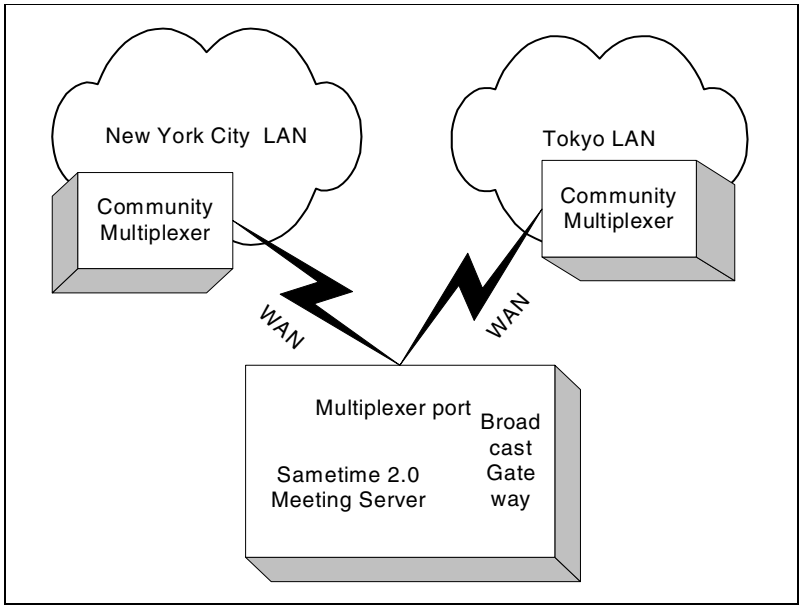


Figure 17. Connecting 2 remote Sametime multiplexers to a single server

This scheme reduces the potential number of community connections that must be maintained from (x) clients on each LAN to 2 community connections over the WAN. This gives you a tremendous reduction in IP overhead management for the server and WAN traffic. The remote muxs handle the large number of connections with each individual client.

2.4.5 Should I use a separate mux?

There are several cautions to consider when utilizing the multiplexers:

- You must still maintain them. They are not a ‘fire and forget’ solution.
- Since multiplexers only manage the community services load, if you have a strong WAN that can handle the network traffic generated, the impact of all your client connections over a WAN may not be felt at all. It may be a better use of hardware to establish more full servers.

2.4.6 Connecting clients to a mux

Each mux is a logical extension of a server, and each mux can only be assigned to one home server. For example - Mux 1, 2, and 3 are all assigned to Server 1. Your clients then set their connections to the address of the mux, and when logging in, the connection data is passed through the mux to its assigned home server. Mux services function exactly as if the mux had never left the server.

You can achive basic load balancing of users across your muxes by utilizing a round-robin DNS or similar system. For example, you can use a single DNS name for your server called “Sametime01.fishnet.com” but have the IP addresses and names of the three muxes (STMux01.fishnet.com, STMux02.fishnet.com, STMux03.fishnet.com) set to be associated with that IP call. When the DNS query is made by the client, they are given one of the three associated IP addresses to connect to. That way users never have to specify which particular mux to connect to.

2.4.7 IP port useage details

Figure 18 on page 42 illustrates the IP communication between core servers and community multiplexers. These are valid no matter where you locate your muxs on the network.

Assume that all community connections to the client from the mux are on port 1533 (the default). Port 1516 is used to maintain server to server awareness, community status, and message exchange. Port 1503 is for meeting data sharing, and port 1352 is used for Sametime meetings scheduling updates.

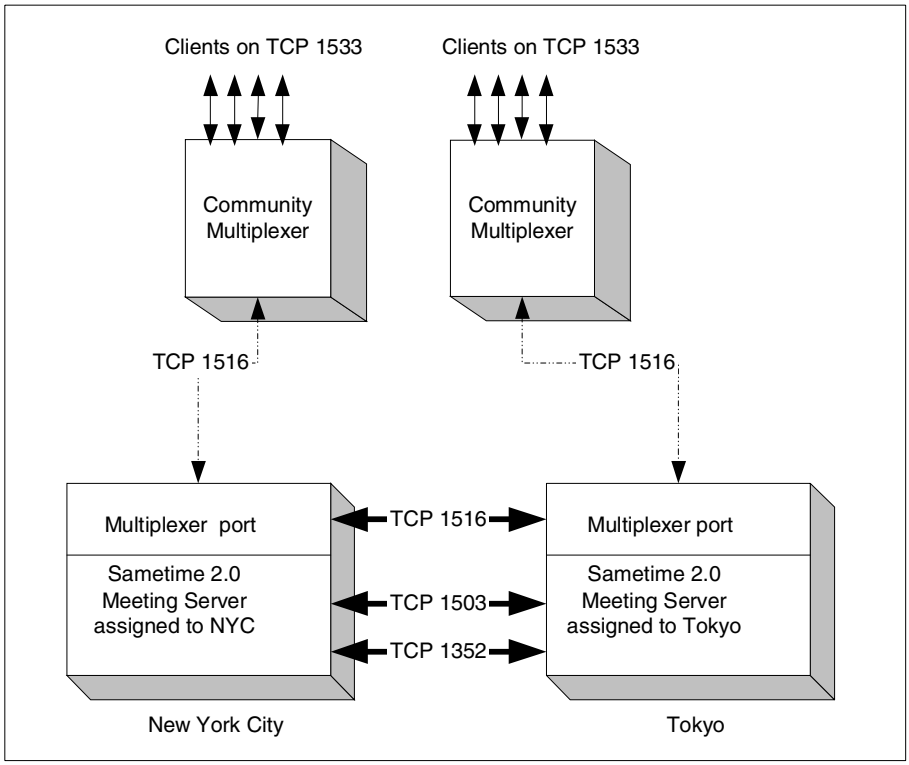


Figure 18. IP port connection detail between server and mux

2.4.8 Broadcast gateway (BG) service

A new feature in Sametime 2.0 is the broadcast gateway. The broadcast gateway allows you to send 1-way data/audio/video streams to large numbers of clients, using a small, lightweight Java client that is dynamically loaded and run on the client. The broadcast gateway feature is a built-in function of a Sametime 2.0 server.

Normally the broadcast gateway looks like Figure 19 on page 43, with broadcast connections to each PC being fed out from the host meeting server. This is very similar in arrangement to how an interactive meeting is hosted on the Sametime core server.

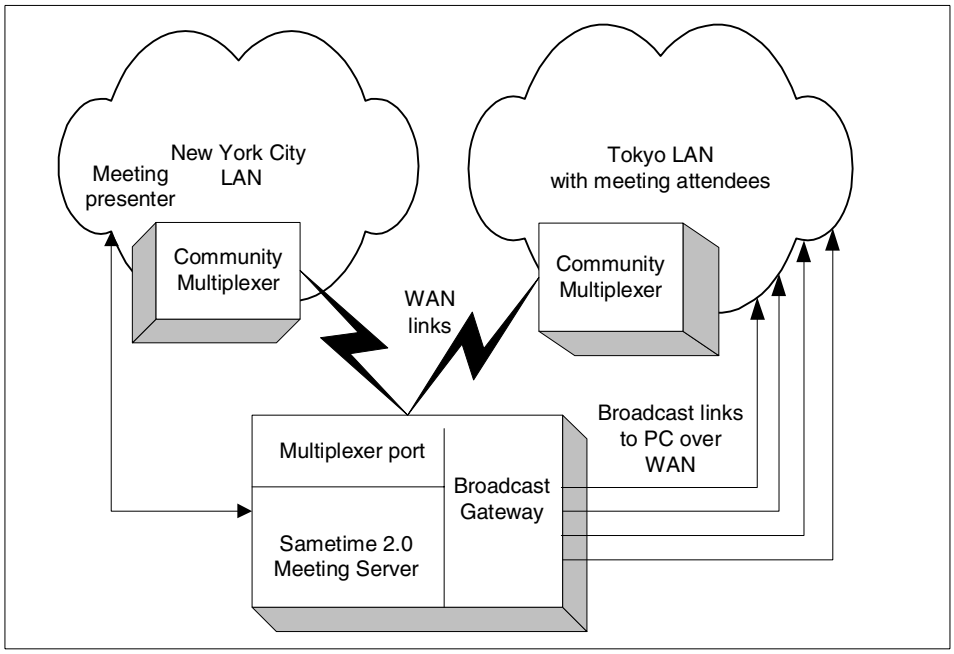


Figure 19. Broadcast gateway in normal use on ST server.

Once a broadcast meeting is downloaded and active, the client PCs on the LAN make their connections directly to the Sametime server broadcast gateway, and begin to receive the media stream.

If you use IP multicast-enabled routers, then you can stream out to very large numbers of clients, with the broadcast gateway serving up the initial feed to each multi-cast router, which then duplicates and retransmits to each connected client.

While using the broadcast gateway to send out 1-way meeting streams is far less taxing on a network than a 2-way connection with the same number of users would be, there are still limits in network capacity and how many outgoing broadcast gateway connection streams can be created.

2.4.8.1 Option: Detached broadcast gateway

As with the community services multiplexer, you can gain some significant network performance by moving the broadcast gateway function off the hosting server and closer to your users.

By moving the gateway closer to the clients, you can avoid having large numbers of individual connections over your WAN, thus avoiding excessive

"hops" that cause transmission lag. In the example shown in Figure 20, it has been determined that almost all broadcast watchers are within the Tokyo LAN, so the gateway will be moved closer to them. For this exercise we will assume there is only one server in use.

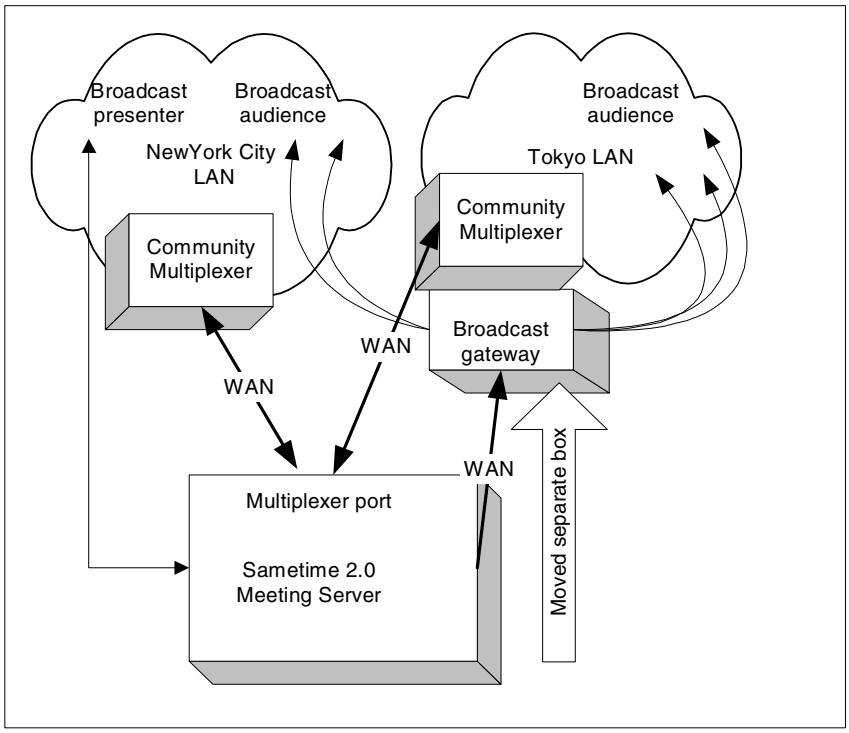


Figure 20. Use of Sametime broadcast gateway moved out from server to be closer to clients.

Note that you can only have one broadcast gateway per Sametime server, so if remote clients on a different LAN section need to receive a broadcast meeting from elsewhere on the network, those users must connect to the broadcast gateway directly (this might not apply to multiple server installations that would be able to provide a broadcast gateway for each LAN area).

While this can be a definite way to improve your broadcast meetings and WAN performance, review and test this option carefully before implementing it.

2.4.9 Establising a separate broadcast gateway server

Caution

This is *not* a normal setup procedure and it is not offically supported. Do this at your own risk.

1. Disable the broadcast gateway on the Sametime server by changing the following registry item:

   `\HKEY_LOCAL_MACHINE\SOFTWARE\Lotus\Sametime\MeetingServer\Services\BroadcastGateway\Enabled`

   This is normally set to 1 in a default shipping Sametime server. Set this to 0 to disable the broadcast gateway from running on this server as a Sametime service.

   Note

   In beta 2 the path was

   `\HKEY_LOCAL_MACHINE\SOFTWARE\Lotus\Sametime\MeetingServer\Services\Service7` with value ServiceDisabled changed from 0 to 1.

2. Configure the Sametime server broadcast gateway IP address/machine-name to be your new machine of choice.
3. Launch Notes on the Sametime server. Open the Sametime Configuration database.
4. Double-click on the BroadcastGateway entry, change Network Address to the IP address of the remote broadcast gateway, and close Notes.
5. Reboot the Sametime server.
6. Collect the following files from the Sametime base directory and move them to a directory on your new Sametime broadcast gateway server.
   - stbroadcastgateway.exe
   - STDiagnostics.dll
   - stgwcommon.dll
   - stgwmediacontrol.dll
   - stgwnetworklayer.dll
   - stgwnetworklayertunnel.dll
   - stgwpiappshare.dll
   - stgwpiimagestream.dll
   - stgwpiwhiteboard.dll
   - stgwrtp.dll
   - stgwthinmcs.dll

- STMemoryManager.dll
- STOS.dll
- STUtilities.dll
- ISRDBG32.dll (BETA 2 note - this file might not be in the final version.)

7. Restart your original Sametime server to effect the changes you've made.
8. Start the newly relocated Sametime broadcast gateway as follows:

   ```
   stbroadcastgateway -install
   ```

   (this will install as an NTService)

   ```
   stbroadcastgateway -start
   ```

   (this will start this newly installed NTService)

Once the broadcast gateway has been installed as an NT service, you can then use normal NT Service mechanisms to start and stop the service.

2.5 Server-to-server networking considerations

Since Sametime services can be distributed across different servers and even across different sites, if you are planning on deploying servers in more than one location to support your organization, these are the items to review.

- Your first priority is to minimize the number of WAN “hops” your data must make to travel from server to client.
- Servers can invite other servers to attend a meeting, and spread the load between them. Users specify to invite other servers when the meeting is booked. Each server relays the meeting data to its attached (home) users attending that meeting.
- Adopt a consistent naming scheme, and update your DNS listing with the fixed addresses assigned to those servers.
- Connecting Sametime servers in different parts of the world is a straighforward process if you already have a Domino environment installed.
- If you do not use Domino, establishing links between servers is a matter of making sure that all servers are aware of each other’s presence. See 1.2.1, “Multi-server Sametime installations” on page 8 for more information.
- Communication between servers is done over a separate connection from what the clients use to connect (tcp 1533 for clients, tcp 1516 for servers), so consider the impact that each connection might have on your network.

If you have a busy WAN, arranging server-to-server links over the WAN will be far more efficient than having individual clients directly connecting over the WAN.

- While Sametime community and text-based IM services will have little impact on WAN traffic, as you introduce more data-intensive services the load goes up significantly. The latency of this can become very noticeable in audio and video services. Despite the best in compression and network speed, multiple hops can reduce any meeting to a disjointed affair.
- Test your links thoroughly before planning any real meetings.

2.5.0.1 Network stability

While we had no good way to test this in the lab, we feel it's worth it to mention this item, since it has been experienced in the real world.

The Sametime system relies on steady connections between clients and servers to maintain community status. If this server link is interupted, the Connect client will make several attempts to reattach before it gives up and reverts to a disconnected state and awaits a manual reconnect command.

Sametime servers will continue to attempt connections to other servers indefinetely.

If you have a network interuption of any kind that prevents updates from getting through, you will have Sametime clients that will be disconnected from the server community.

After this happens, Sametime clients will attempt a reconnection. When the network reopens, the result is a surge in authentication requests and buddy list updates against the servers. If the surge is big enough, users may have long waits before all disconnected clients are restored.

When investigating your network, you may want to set up network sniffers and probes to test any networking drops or congestion issue.

2.6 Internet or firewall connections

While the initial focus of installing Sametime tends to be internal, there are many situations when you will want to be able to included external users in your Sametime meetings, or to enable your website with Sametime functions.

Sametime can be set up to allow access through your network firewalls. We highly recommend that you have a separate server established for this purpose, both for security and for ease of configuration.

A detailed example of how to set up access over the firewall is in Chapter 6, “Deploying Sametime on the Internet” on page 149.

2.7 Directory services

Since Sametime is a person-to-person tool for teaming and collaboration, you will need to manage IDs, as well as provide a directory service so Sametime users can find others online. This section will discuss the three types of directory services you can use in Sametime.

The details of setting up each directory type can be found in the *Sametime 2.0 Administrators Guide* Lotus Notes database, which ships with the product.

2.7.1 Web-only Sametime directory

The first option for directory services is referred to as a “Web-based” or “stand-alone” directory. The directory is maintained by Sametime, and is completely independent of any other directories you may have in your business. It can be opened to allow self-registration via your Sametime server homepage on the server. The directory is an R5 Domino directory in format, but it does not maintain any connection to any other Domino directories that may exist in your organization.

Its benefits are:

- Instant registration
- Only Sametime users are in it
- Light weight directory
- Can be maintained from a Web client or Notes client

While allowing users to self-register is permitted, this would generally not be a recommended practice for most business installations.

Why? Most business people would want some assurance that the person they are communicating with is really who they say they are. Think about it: do you want someone to pretend to be the CEO online? It’s also important for larger organizations, when a new Sametime contact is made, to give some assurance that this is a legitimate user contacting you since you may never have met them in person.

If you choose not to allow self-registration, the system administrator will have to create all names and passwords in the directory, along with all resets and password management of the IDs in the Sametime directory.

A self-registration system would be recommended for open Internet discussion and chat websites, where user validation would be less important.

To set up a stand-alone Sametime directory, you must specify this when installing the Sametime server. For more information on setup options, see the Sametime Installation Guide or the Sametime Administrators Guide, and Chapter 1 of this redbook.

2.7.2 Domino directory

The next option for Sametime directory management is to utilize or establish a Domino directory service. This is the most integrated of options, especially if you have an existing Domino server system in place. To make use of it, during the Sametime server installation, Sametime simply creates a full replica of the main Domino directory. This is used from then on, and is updated on the replication schedule you operate in the Domino environment.

The benefits of using a Domino directory include:

- Users already have names and passwords.
- Domino administration methods are already set up.
- It stays up-to-date with Domino through replications.
- It is the easiest way to take advantage of third-party applications and their API function calls to Domino.

When using a Domino directory, you must populate the Sametime Server home field in the Domino directory in two situations: when you plan to use more than one server, or when you plan to make use of Sametime-enabled applications located on other Domino servers.

2.7.3 LDAP directory

The option of using LDAP directories (such as IBM SecureWay Directory or Netscape Directory Server) is a new feature in Sametime 2.0. Many organizations are now establishing LDAP directory systems that allow applications to use a single resource for ID and passwords and other essential information.

Sametime servers will access an LDAP service on the Sametime client's behalf if the following criteria are met:

- A *home Sametime server* field is in your LDAP schema (for 2 or more Sametime servers, or for applications using Sametime API).

- Anonymous binding to LDAP servers is permitted by LDAP. (You can provide an ID and password for LDAP access in the server configuration file, STCONFIG.NSF, but at the time of writing, it is not know if this will be an active feature or not in the final code.)
- You set up the Sametime server at installation to use LDAP as its directory source.

You can access multiple LDAP directories through Sametime, assuming they all have the same directory schema for user and group listings. The connections to each LDAP server can be set up in the Sametime Administration Web control console.

Utilizing LDAP as your Sametime directory service has great benefits as far as centralized management goes, but it presents some special access and control issues that need to be considered:

- You cannot manage LDAP directories from Sametime. Any changes required in the directory must be done through the LDAP processes set up in your choice of software.
- The LDAP directory cannot be “browsed” for users, only searched on specified criteria and fields set up in the Sametime server.

2.7.3.1 Domino via LDAP

If your Domino directory system is set up to provide LDAP, it may be to your advantage to use it. Accessing Domino over an LDAP connection will save you from keeping another copy of the Domino directory on the Sametime servers. In the event of very large Domino directories, this can be a good way to conserve Sametime server CPU, disk, and RAM capacity.

2.7.3.2 Considerations for using LDAP

This section discusses a few items to keep in mind when choosing LDAP for your Sametime directory services. For more information on how to install and administer LDAP servers, consult the documentation for your LDAP server.

Pre-install

Sametime servers act as anonymously binding LDAP clients. (A field for LDAP ID/password does exist in STCONFIG.NSF, but it is not visible to the Sametime Administration panel.) Sametime clients do not directly access LDAP services. All results are passed back to the client in a Sametime format.

The LDAP directory must have a password in the userPassword field. (This is usually a default in any LDAP installation.) This password must be in use and updating from your LDAP services.

If you plan on using more than one Sametime server or Sametime-enabled applications, you *must* add a field to your LDAP directory to hold the Sametime home server name assigned to each user, and then populate this field via your LDAP management system. If using Domino via LDAP, you must make the home server field available to Sametime LDAP queries.

During the install
LDAP must be chosen when first installing your Sametime server. Select "Web only Community" and "LDAP Directory" during the install steps.

You must know the IP addresses of your LDAP server, and whether you are using SSL encryption or not. If you are not, the default port is 389. If you do use SSL, the default port is 636.

Post-install and administration
After the install is complete, you must use the Sametime Administration application (Administer Sametime) to set up the details for LDAP access.

You can add additional LDAP directories, as long as all have the same schema for names and groups.

You must specify the search order for each LDAP directory in use. We suggest you make your primary server the first one searched. If no results are found, then each remaining server will be queried in order.

All LDAP servers share a common Sametime authentication and query formula. You cannot create unique queries for each LDAP directory.

If you use more than one Sametime server, you must add the Sametime home server field into your Authentication query. This is so Sametime knows to which server to connect to obtain your specific Sametime information.

You must add/modify the query statement to match the LDAP attributes you wish to use for validation. The default query statements should work for most installations, but consult your LDAP administrator before creating your query.

The STCONFIG.NSF database on the Sametime server holds most of the data used in Sametime configuration. However, LDAP also makes use of Directory Assistance (DA.NSF). If you are having problems connecting to the LDAP server, make sure that DA.NSF has the correct values included also.

If changes made to the LDAP settings in Sametime Administration, you must restart the Sametime server for the changes to take effect.

For complete details on setting up LDAP access, see the Sametime Administrators Guide.

2.8 Upgrading from Sametime 1.5

If you are installing Sametime 2.0 on top of existing 1.5 servers and applications, consider the following:

Do you have any applications that are using Sametime APIs to obtain data from 1.5 servers (for Web page presence applications for example)? If so, the 2.0 API will not be compatible with the 1.5 servers.

Will you be able to upgrade all your 1.5 clients to 2.0? Issues of code distribution must be addressed.

Sametime 1.5 Connect clients are capable of connecting with Sametime 2.0 servers for community services, text IM, and meetings. However, they will not be able to use the audio/video functions until you upgrade their client code to 2.0. The Meeting Room Client (MRC) will work for 1.5 users who access the meeting via a 2.0 server website.

Sametime 1.5 clients will not be able to use 2.0-level API applications.

A detailed list of steps for migrating existing Sametime installations is in the Sametime Administrators Guide.

2.9 Workplace/ Human issues

Sametime (if you are new to it) introduces some interesting business and workplace issues beyond anything that software can effectively deal with. While we make no claim that the issues described here will be pertinent to your business, Sametime is different enough from other types of communication tools that some of our experiences might be of interest to you. The areas of interaction that were affected in our environments included the following:

- Team dynamics
- Business-critical application
- Impact on phone use/e-mail
- “Lurking” and privacy

2.9.1 Team dynamics

Sametime has been observed to change the way even people who are physically close to each other work with one another. Many users have reported that they now send an IM to ask a casual question, or to find out if the person is really in the office. In short - they don't get up from their desks as much.

There has also been a noted effect from the lack of context in messages. If you close a chat session, and another comment is sent later, you may not have a recollection about the original topic of discussion. We have found that short references to the topic help keep things clearer.

2.9.2 Business-critical application

Instant messaging has become as important to many users as the telephone and e-mail have. Many users have made it the most important way to work with team members, especially on time-sensitive items. And it has had a "time compression" effect on messages. We often don't expect an immediate reply to our e-mails and phone messages, but we do expect anyone online and active to respond quickly.

It has also resulted in users noticing if IM fails to work even for a few minutes.You will need to consider what level of support you will have to provide once your users incorporate Sametime into their work day.

2.9.3 Impact on phone and E-mail use

While no quantitative studies have been done, evidence suggests that using Sametime has reduced the number of e-mails sent in day, and even cut the number of phone calls made. Since IM uses already existing networking, and has no direct costs for each message sent, the savings in resource can be a significant benefit of using IM technologies. The elimination of many "one line" e-mails in your inbox can also be a serious mental benefit. The turn-around time for answering is also greatly reduced when using IM rather than e-mail.

Realize that IM is not a replacement for phone, e-mail, or in-person communication. We've found that it works best for short, simple topics that do not need reference information (as an e-mail can contain), or personality and emotion (as might be best done in person or on the phone), which can be needed when dealing with some topics.

2.9.4 'Lurking' and data privacy

Sametime and other IM applications offer a new way for teams to monitor who is active and who is not. While in all reality this can mean nothing since a user can be active on Sametime, but asleep at the desk, it's still creates a perception that many people can have about how and when you are online.

Sametime also allows for text conversations to be captured by any participant to a text file. There is no direct method for capturing audio and video in Sametime meetings. This would be possible with any number of PC software programs, and a Sametime API to allow a capture/replay of a meeting is under development.

2.10 Recommended hardware

This secton describes the system requirements for the Sametime server and client computers.

2.10.1 Server requirements

Our recommendation is based on a single server to be used by a group of 500 regular users.

Table 9. Server requirements and recommendation

Server Requirement	Minimum (will work)	Real recommendation
CPU	Single Pentium II 300 MHz	Dual Pentium II 500 MHz
Operating System	Window 2000 Server or Windows NT 4.0 SP5	Windows 2000 Server or NT 4. SP5
Memory	128MB min, 256MB rec	512 MB min 1 GB rec
Disk Free	300-500MB	2-4 GB
Swap	64MB	128MB
Networking	TCP/IP	TCPIP
Browser level	Netscape 4.5 or Internet Explorer 4.01 SP2	Netscape 4.5 or Internet Explorer 5

Important note: Ensure that the Administrator who is logging on to Windows NT or Windows 2000 to perform the installation has full administration rights. If not, Sametime will not be installed properly.

2.10.2 Client requirements

Below are the minimum and recommended requirements for a Sametime client. Our “real recommendation” is based on our collective experiences during testing, using audio and video. If you are using only whiteboard and screen shares, the minimum will work.

Table 10. Client requirements and recommendation

Server Requirement	Minimum (will work)	Real recommendation
CPU	Pentium II 233 MHz	Pentium II 233 MHz
Operating System	Windows 95 OSR2, Windows 98, 98SE, Windows NT 4.0 SP5 Windows 2000 Professional	Windows 95 OSR2, Windows 98, 98SE, Windows NT 4.0 SP5 Windows 2000 Professional
RAM	Win95,98 - 64MB Win NT/2000 - 96MB	Any level you feel runs fast enough to handle several programs at once - we suggest 128-256 MB
Disk Free	10 MB	10 MB
Swap	Windows defaults	Windows defaults
Networking	TCP/IP	TCP/IP
Browser level	Netscape 4.5 or Internet Explorer 4.01 SP2 (or higher)	Netscape 4.7 or Internet Explorer 5 (or higher)
Audio	Windows standard audio services	Windows standard audio services
Video	Windows standard video services	Windows standard video services

Additional client requirements for audio/video:

Sound card: A full-duplex sound card is required to participate in interactive audio/video meetings. A half-duplex sound card is required to enable a user to listen to an audio meeting that is broadcast by the Sametime Broadcast Services.

Microphone and speakers: High-quality microphones are recommended. Avoid microphones with on and off switches unless they are of high quality. A headset that contains a boom microphone performs best. If a desktop microphone is used, a unidirectional dynamic microphone with outside power

supply is preferred. Laptops with built in microphones and speakers will work, but are prone to feedback.

Camera: A high-quality USB or PCMCIA PC camera is recommended (do not use parallel port cameras). A camera is optional. Users who do not have a camera can still participate in an audio/video meeting. These users can see video images displayed in the Sametime Meeting Room client. When a user without a camera speaks, no video image is displayed in the video component of the Meeting Room client.

Video capturing software: The Sametime client uses the standard Win 32 API interface for video capture. You can test your camera for compatibility by using any one of several video capture utilities such as VidCap by Vista Imaging Software, a package often supplied with your camera when purchased.

Another good test is to use Microsoft Net Meeting (since it's installed on almost every Windows PC you may as well use it for something). If you can see a picture in the "My Video" window, you have a working camera for Sametime.

Chapter 3. Performance considerations

This chapter focuses on performance considerations for deploying Sametime 2.0. We provide information on each codec that Sametime uses for audio and video, define the term *acceptable performance*, and describe techniques to optimize the performance of Sametime 2.0 in your organization.

3.1 Codecs used by Sametime

A *codec* is an algorithm that performs compression and decompression of data. Typically this data is either audio or video. Sametime uses the H.263 codec for video. The G.711 and G.723 codecs are used for sound compression.

Each of the above codecs are part of the H.323 standard which has been issued by the International Telecommunication Union (ITU); the H.323 standard can be purchased from the ITU's website at `www.itu.int`

H.323 is an umbrella recommendation from the ITU that sets the standards for multimedia communications over local area networks that do not provide a guaranteed Quality of Service (QoS), for example, the Internet.

3.1.1 H.263

This is the only codec used for video in Sametime 2.0 and is a standard video-conferencing codec. It is optimized for low data rates and relatively low motion. The primary goal of H.263 is to provide good quality video below 64 Kbps.

You can adjust the bitrate from 16 kbps to 128 kbps, but this setting will only take effect during a broadcast meeting.

3.1.2 G.711

The G.711 codec is optimized for compression of speech data that is transmitted over links with a minimum speed of 64 kbps. By default Sametime will only use this codec when all users are connected via a LAN.

Audio compressed with G.711 will use 64 kbps in one direction.

3.1.3 G.723

This codec is optimized for compression of speech data that is transmitted over standard telephone lines and is optimized for real-time encode/decode.

Real-time encode/decode can be resource intensive, which is why Sametime 2.0 requires a relatively high-end workstation.

Generally this codec will utilize 6.3 kbps in one direction.

3.1.4 Configuration options for codecs

End users cannot explicitly choose the codec they wish to use.

When users schedule a meeting they can choose whether or not users are attending via a modem. This is set to true by default. If this setting is left on, then the G.723 codec is used for sound compression and a bit rate of 16 kbps is used for video transmission.

If your meeting consists of users that are attached to a LAN, you can deselect the “People are attending using a modem” option. This means that the G.711 codec is used for sound compression and a bit rate of 64 kbps is used for video transmission.

The settings above represent the defaults and can be configured via the Sametime Administration Client. Administrators can choose to use either the G.711 or G.723 codec over either connection type with a combination of bitrates ranging from 16 kbps to 128 kbps.

3.2 Bandwidth usage

Bandwidth usage is a concern with any application deployed across a network.

Many customers may have concerns about the implications of deploying an application on their networks that contains streaming multimedia technology. The developers of Sametime anticipated this concern and provided a model of control that is flexible, yet absolute.

It is possible to deploy Sametime 2.0 without the audio/video components and still take advantage of the improvements in community services and meeting services offered by version 2.0 over those available in version 1.5. If administrators wish to deploy the full Sametime server they are also given the option to limit the number of active audio/video meetings.

3.2.1 Estimating bandwidth usage

The following sections provide information on the bandwidth usage of the G.711 and G.723 audio codecs and demonstrate how we arrive at our calculations.

3.2.1.1 G.723

The G.723 codec uses 6.3 kbps of data. It is important to remember that this is a per second measurement. However, transmitting one second intervals of audio data will not result in a natural conversation, since the person receiving this data will be on a one second delay. To facilitate speech that flows more naturally, Sametime Multimedia Services breaks the audio data into either 20 ms or 30 ms chunks, called frames, depending on which codec is used. So one second worth of audio would be broken into 33.3333 frames of 24.2 bytes for the G.723 codec. For the G.711 codec, once seconds worth of audio would be broken into 50 frames of 163.8 bytes per second.

Refer to Table 11 for a quick summary of bytes per second that audio will utilize when compressed with G.723. Note that each packet containing frames will have a 40 byte overhead for protocol information.

The Sametime administrator can specify the number of audio frames per packet. This has an affect on the quality of the audio end users will hear and on bandwidth utilization. In general, if there are more frames per packet the network bandwidth utilization will be lower, but audio quality will be more susceptible to packet loss.

Table 11. Bytes per second G.723 will use on a single audio stream

Frames per Packet	Frame Payload (in bytes)	Protocol Overhead	Packet Size (in bytes)	Bytes per second of audio
1	24	40	64	2133
2	48	40	88	1467
3	72	40	112	1244

3.2.1.2 G.711

The G.711 codec uses 64 kbps of data. Sametime Multimedia Services uses a 20 ms frame technique with this codec to provide a more natural flow of speech. However, each frame will contain 245 bytes of data under the G.711 codec.

Refer to Table 12 for a quick summary of bytes per second audio will utilize when compressed with G.711. Note that each packet containing frames will have a 40 byte overhead for protocol information.

Table 12. Bytes per second G.711 will use on a single audio stream

Frames per Packet	Frame Payload (in bytes)	Protocol Overhead	Packet Size (in bytes)	Bytes per second of audio
1	164	40	204	10200
2	328	40	408	20400
3	492	40	612	30600

3.2.1.3 Calculations

How did we arrive at the figures in the previous tables? Following is an explanation. If you are already comfortable with the calculations and results, you may wish to skip this section.

A millisecond (ms) is 1/1000 of a second (one one-thousandth). Therefore there are 1000 ms in a single second.

Sametime Multimedia Services breaks audio data using the G.723 codec into 30 ms chunks. This means that one second worth of audio is broken up into the following number of frames:

$$\frac{1000\,ms}{30\,ms} = 33.333333\,Frames$$

Given the number of frames per second, we know that when using the G.723 codec we are transmitting 6.3 kbps. So per second we transmit the following number of bits:

$$(6.3 \times 1024) = 6451\,bits$$

We convert our bits back to bytes by dividing by 8. We can then determine the payload of each frame:

$$806.4\,bytes \div 33\,Frames = 24\,bytes$$

The calculations for the G.711 are the same, but the chunk size is 20 ms and the data transmitted per second is 64 kbps. Therefore, the formula would look like this: ((64 * 1024)/8) / (1000/20) = 163.84 bytes per second.

3.2.1.4 Implications of the frames per packet setting

In addition to the compressed audio data there are also 40 bytes of packaging and transport headers that are added to each packet transmitted over the network. This is illustrated in Figure 21.

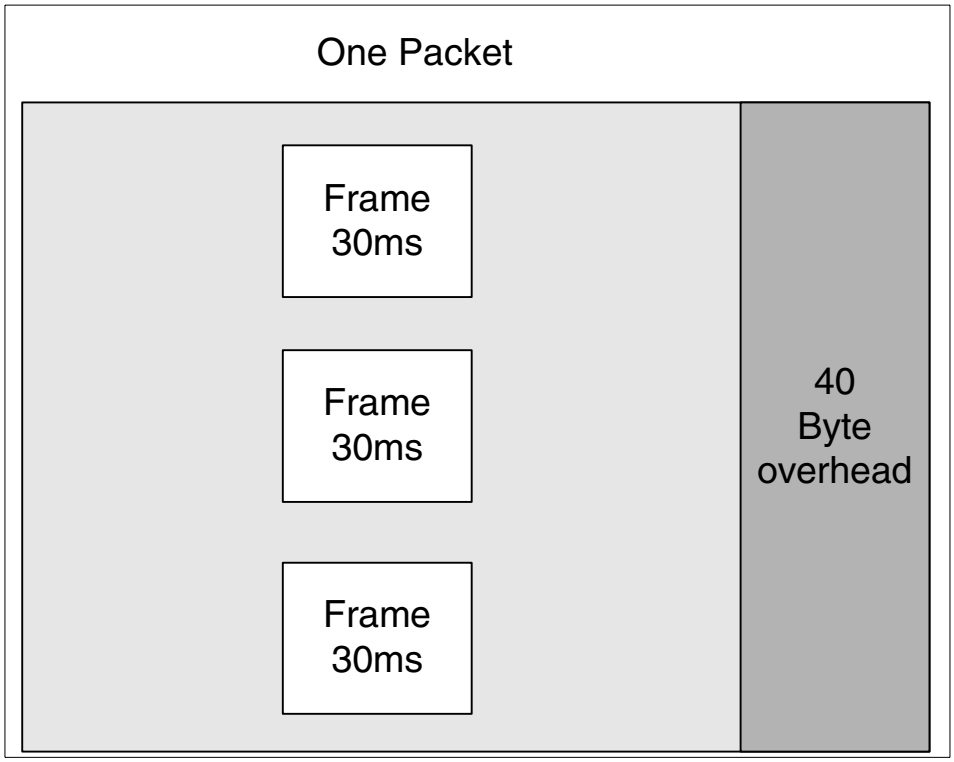


Figure 21. Three frames in a packet with 40 byte overhead

Although this overhead doesn't sound like much, it does add up. By default, the Sametime server transmits three audio frames (90 ms) per packet, which means for every second of audio that is transmitted we must send roughly 11 packets. With a protocol overhead of 40 bytes per packet this means that for every second of audio sent we are also sending 440 bytes of overhead. These calculations only concern 1 stream.

If we reduced this to one frame (30 ms) per packet for each second of data transmitted, we would have 33 packets, which is around 1.3 kb in overhead.

Now in a five person automatic microphone meeting we have 10 streams of audio. So for a five person meeting we have 13 kbps of protocol data alone.

3.2.1.5 Calculating the number of audio streams

Our calculations in the previous sections are all based on a single stream. Now we can establish a formula to estimate the amount of bandwidth we will require per *meeting*.

First we need to calculate the number of streams. The number of streams can vary based on the microphone mode of a meeting. In “request microphone mode” the number of streams is determined by simply counting the number of participants. This type of meeting will use considerably less bandwidth than an “automatic microphone” meeting. See Figure 22 for an illustration.

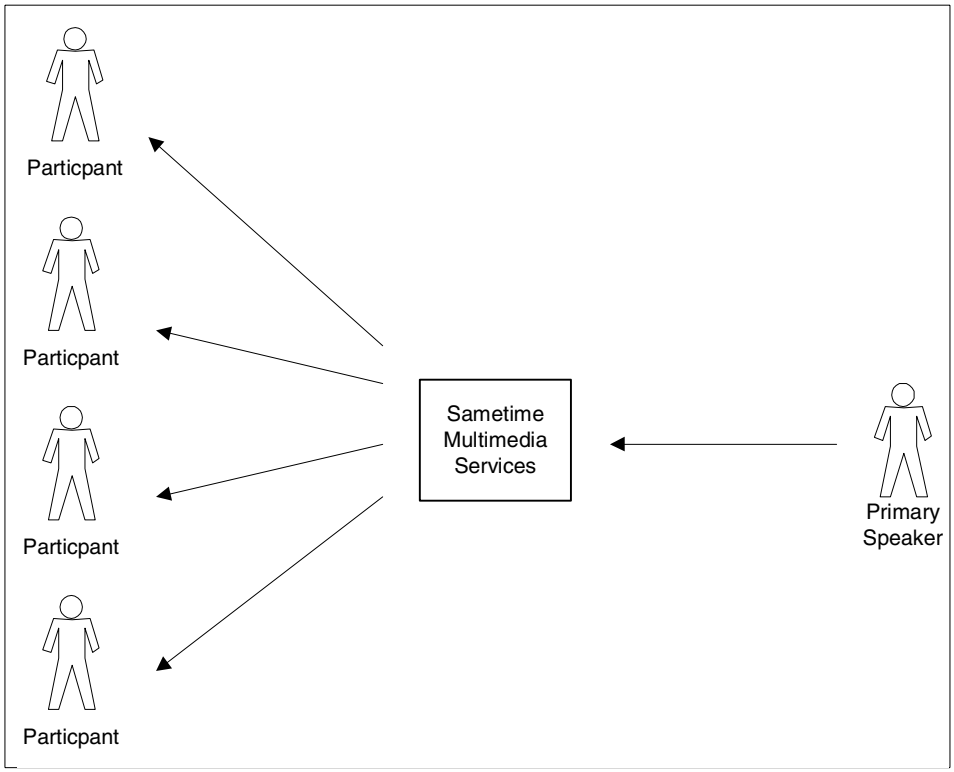


Figure 22. Number of audio streams when using request microphone mode

For example, a five person request microphone meeting using the G.723 codec will consume around 6220 bytes per second of bandwidth, which is equivalent to 48.6 kbps.

An automatic microphone meeting consists of a primary and a secondary speaker. Both the primary and secondary speaker send one stream of audio and receive one stream of audio, since they do not hear themselves. Every other participant in the meeting receives both the primary and secondary audio stream. This means the number of streams for an automatic microphone meeting is derived by multiplying the number of participants by two. As illustrated in Figure 23, the primary speaker's stream is represented by the dashed arrow and the secondary speaker's stream is represented by the solid arrow.

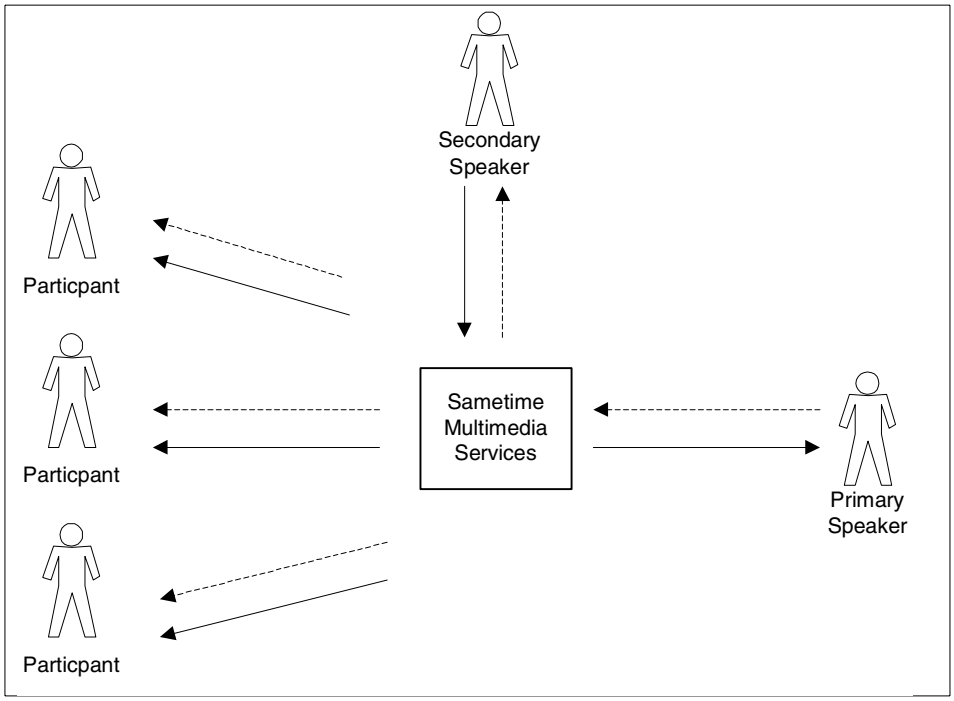


Figure 23. Number of audio streams when using automatic microphone mode

The same five person meeting from the previous example, but using automatic microphone mode, will consume around 12440 bytes per second of bandwidth, which is equivalent to 97.1 kbps, roughly double that of a request microphone meeting.

3.2.1.6 Calculating audio bandwidth for a given meeting

Now that we know how to count the number of streams per meeting and the bandwidth utilization per second we can summarize all of the information with the following formula:

$$Bandwidth = kbps \times participants$$

The numbers you have to use for the kbps variable will differ depending upon the codec, frames per packet, and the microphone mode you are using. Refer to Table 13, which contains the numbers for the default three frames per packet setting.

Table 13. Bandwidth estimation for 3 frames per packet.

Microphone Mode	G.711	G.723
Automatic microphone	134.54 * paticipants	19.42 * participants
Request microphone	67.27 * participants	9.71 * participants

Table 14 contains the values for the two frames per packet setting.

Table 14. Bandwidth estimation for 2 frames per packet.

Microphone Mode	G.711	G.723
Automatic microphone	138 * paticipants	22.92 * participants
Request microphone	69 * participants	11.46 * participants

Table 15 contains the values for one frame per packet.

Table 15. Bandwidth estimation for 1 frame per packet.

Microphone Mode	G.711	G.723
Automatic microphone	148.42 * paticipants	33.32 * participants
Request microphone	74.21 * participants	16.66 * participants

Using the values from the preceding tables, if we have a meeting that is using automatic microphone, uses G.711, uses the default 3 frames per packet setting and contains 10 participants, it will use the following bandwidth:

$$134.54 \times 10 = 1345.4$$

This means that the described meeting will use 1.31 Mbps in total network bandwidth for audio traffic.

3.2.1.7 H.263

Measuring the amount of bandwidth utilized by video in a Sametime meeting is far less complex than that of audio. This is because Sametime Multimedia Services only transmits video for the active speaker, so you only need to multiply the current video bitrate by the number of participants in the meeting to come up with the total network bandwidth usage.

The H.263 codec allows the Sametime administrator to specify either 16 kbps, 32 kbps, 64 kbps or 128 kbps for video bitrate.

Consider the following example: a meeting with 10 participants and a video bitrate of 64 kbps will use a total network bandwidth of 640 kbps. This result would be an absolute worst case and would only occur if the user transmitting the video was moving erratically and often.

3.3 Administration settings affecting audio/video

The following administration settings will affect the audio/video performance of your Sametime installation.

3.3.1 Default settings for modem and LAN users

Administrators have absolute control over the codec and throughput used for a given connection. This control is exercised from the Connection section of the administration client. By default, the modem connection will use the G.723 codec, have a video bitrate of 16 kbps, and send three audio frames per packet.

The following settings can be adjusted by the Sametime administrator for each connection type:

- Audio bitrate
- Video bitrate
- Screensharing bitrate - broadcast meetings only
- Whiteboarding bitrate - broadcast meetings only
- Jitter buffer
- Audio frames per packet

The Sametime administrator can also specify the default connection type when meetings are created, as shown in Figure 24 on page 66.

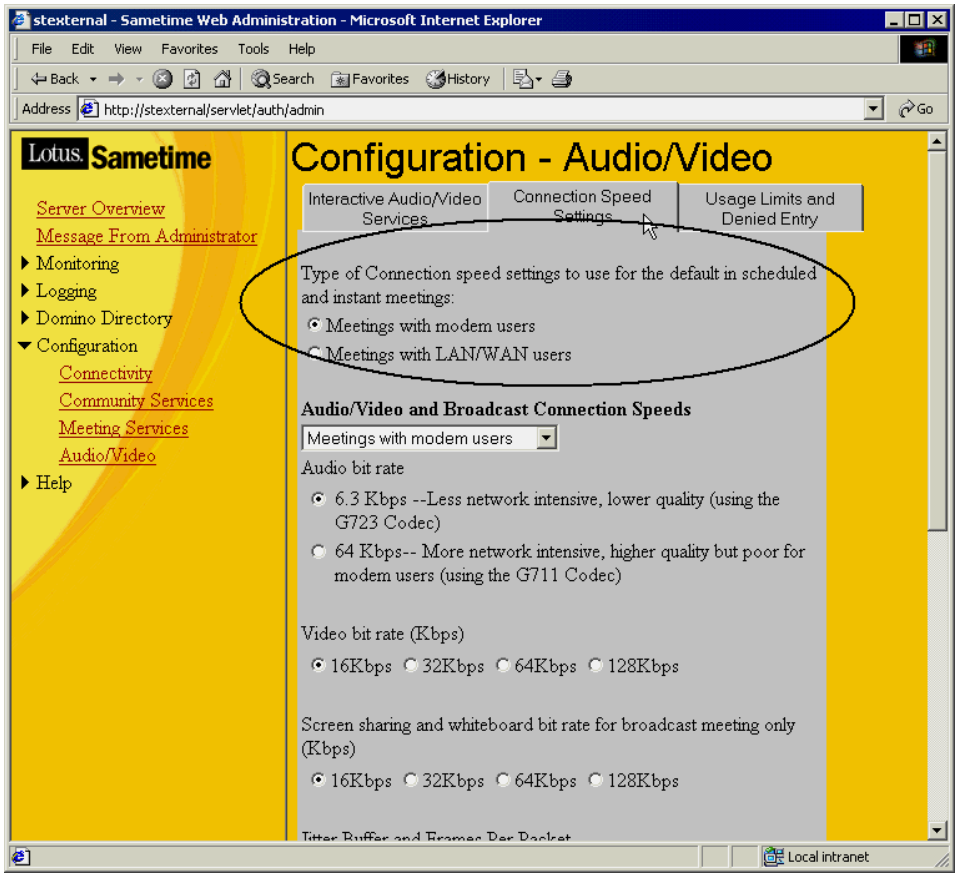


Figure 24. Setting the default connection type for meetings

By default, all meetings will use the modem connection speed settings unless the person creating the meeting unchecks the “People are attending using a modem” checkbox. When this box is unchecked, the settings for the LAN connection will be used. Figure 25 on page 67 shows how this will appear in the Sametime Meeting Center.

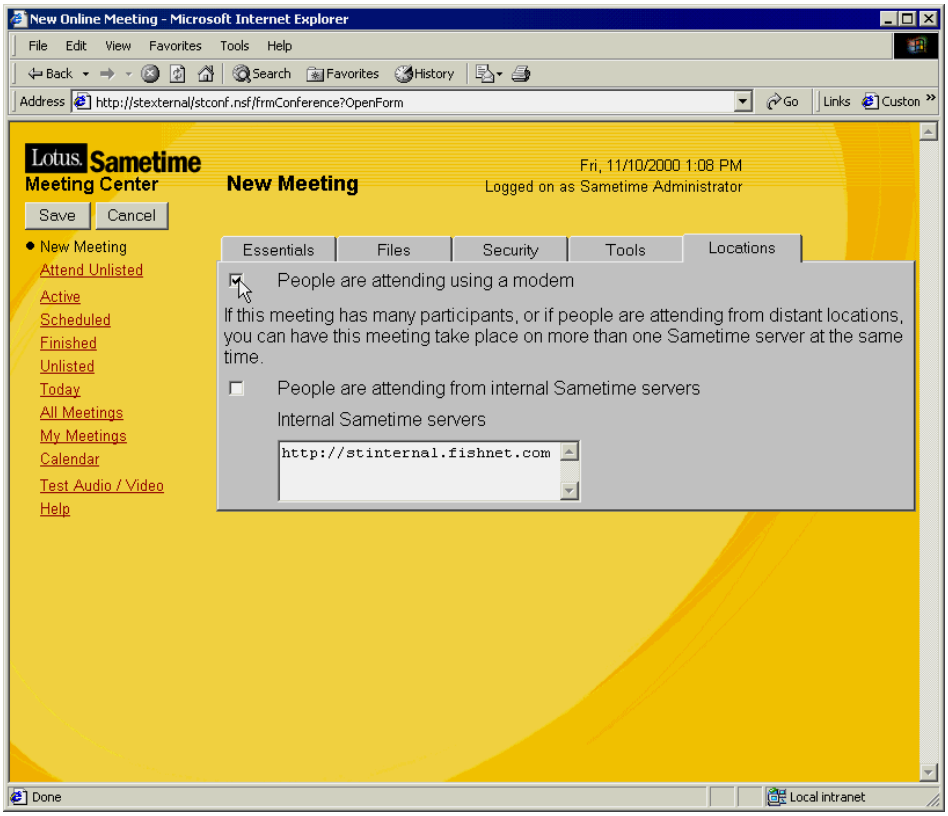


Figure 25. End user specifying the connection type for a meeting

Before changing these settings you must first know the slowest connection speed you are supporting. For example, if you are supporting a minimum of 56 kbps you should not set a video bitrate of 64 kbps.

To change these settings perform the following steps:

1. Open the Sametime administration client by clicking the “Administer the server” link on the Sametime meeting center homepage.
2. A new browser window containing the administration client will be launched.
3. Expand the Configuration link and select Audio/Video. Your screen should now look like Figure 26 on page 68.

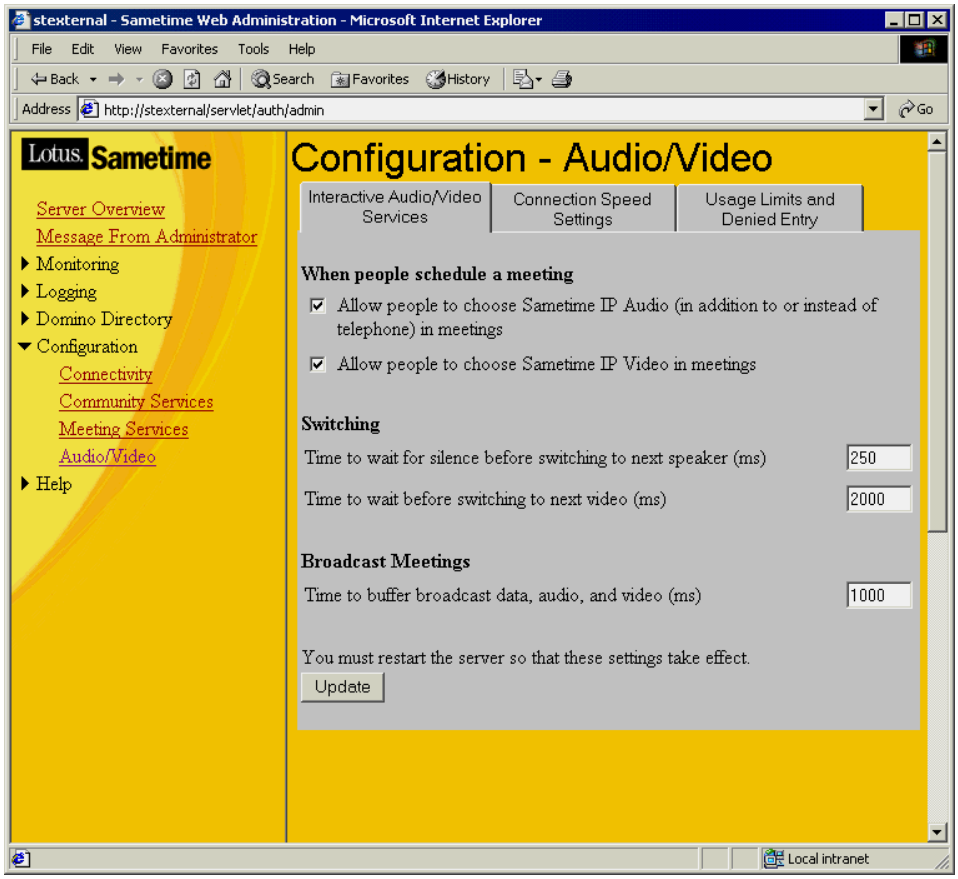


Figure 26. Initial audio/video configuration screen of the administration client

4. Click on the Connection Speed Settings tab to get the screen shown in Figure 27 on page 69.

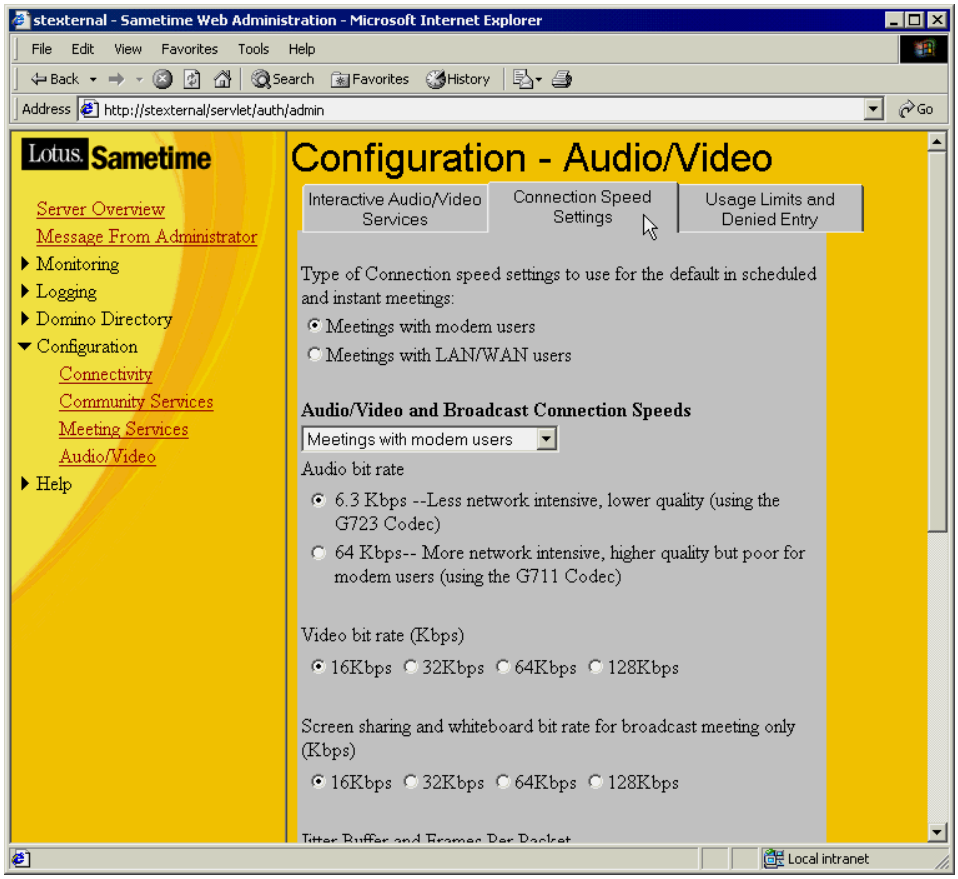


Figure 27. Connection speed settings tab

5. Choose the connection type, either modem or LAN,that you want to set up the codec and video bitrate for. Refer to Figure 28 on page 70.

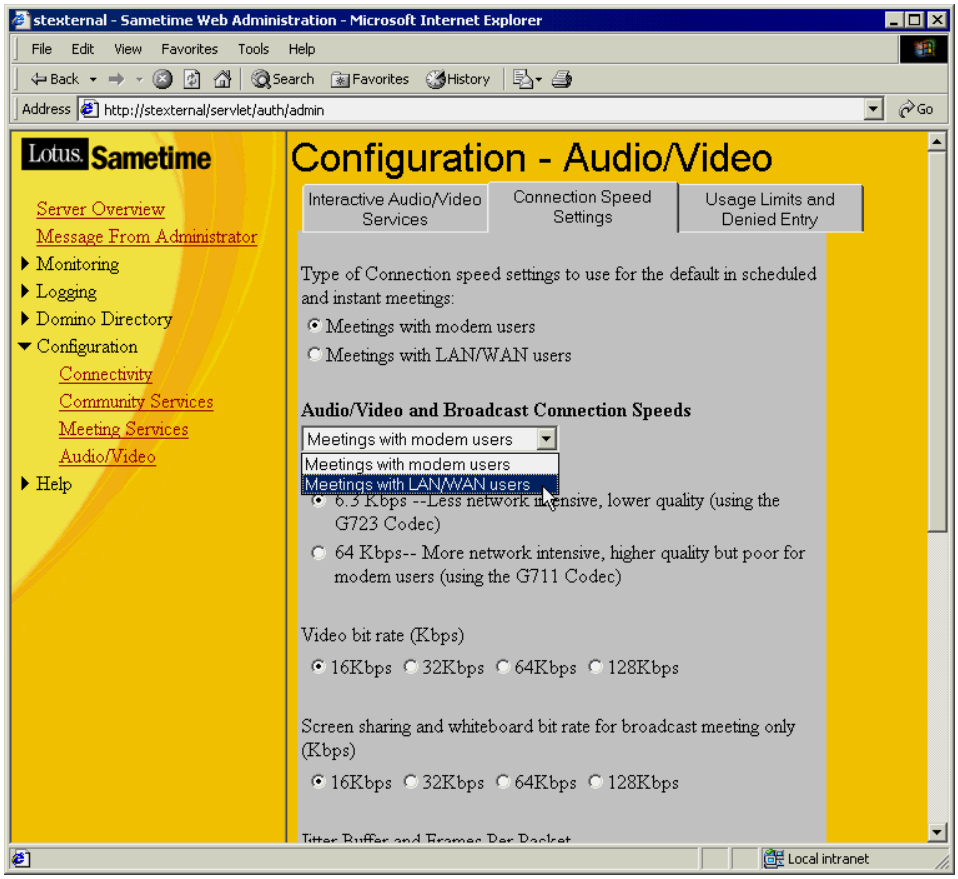


Figure 28. Choosing the connection type

6. Once you have made your changes, be sure to click the Update button and restart the server so they take effect.

3.3.2 Switching

Switching is used during a meeting that uses automatic microphone mode. The “Time to wait for silence before switching to next speaker” field controls how long the server will wait when it detects that the active speaker has stopped talking before switching the “Primary Speaker” assignment to the active “Secondary Speaker.” This setting helps prevent premature switches when the speaker pauses speaking for a moment. The default value for this setting is 250 ms.

The “Time to wait before switching to next video” field tells the server how long to wait after the “Primary Speaker” switch before video is switched to the new “Primary Speaker.” The purpose of this setting is to prevent the video from quickly chopping back and forth if two people are engaged in a “short sentence” converstion such as using phrases like “right,” “yes,” or “OK.” The default value for this setting is 2000 ms or 2 seconds.

These settings are global and specific to a single Sametime server. Under load this will result in high CPU usage.

To change these settings perform the following steps:

1. Open the Sametime administration client by clicking on the “Administer the server” link on the Sametime meeting center homepage.
2. A new browser window containing the administration client will be launched.
3. Expand the Configuration link and select Audio/Video. You should now see the scrren shown in Figure 29 on page 72.

Figure 29. Initial audio/video configuration screen of the administration client

4. In the Switching section on the Interactive Audio/Video Services tab, change the fields to the values you would like to specify. Remember that these settings are in milliseconds.
5. Click the Update button and restart the server for the new settings to take effect.

3.3.3 Jitter buffer

This setting specifies the amount of audio/video data the Sametime Meeting Room client will buffer before playing to the client.

You can use this setting to minimize the effects congestion and other adverse network conditions will have on the quality of audio and video. Network congestion can result in delayed packets or cause packets to arrive out of

order. This will cause garbled speech or jittery speech, hence the name jitter buffer.

Briefly buffering packets before they are played to the client provides a window of time where missing packets can arrive, thereby reducing the jitter effect.

To set the jitter buffer, perform the following steps:

1. Open the Sametime administration client by clicking on the “Administer the server” link on the Sametime meeting center homepage.
2. A new browser window containing the administration client will be launched.
3. Expand the Configuration link and select Audio/Video. You should now see the screen shown in Figure 30.

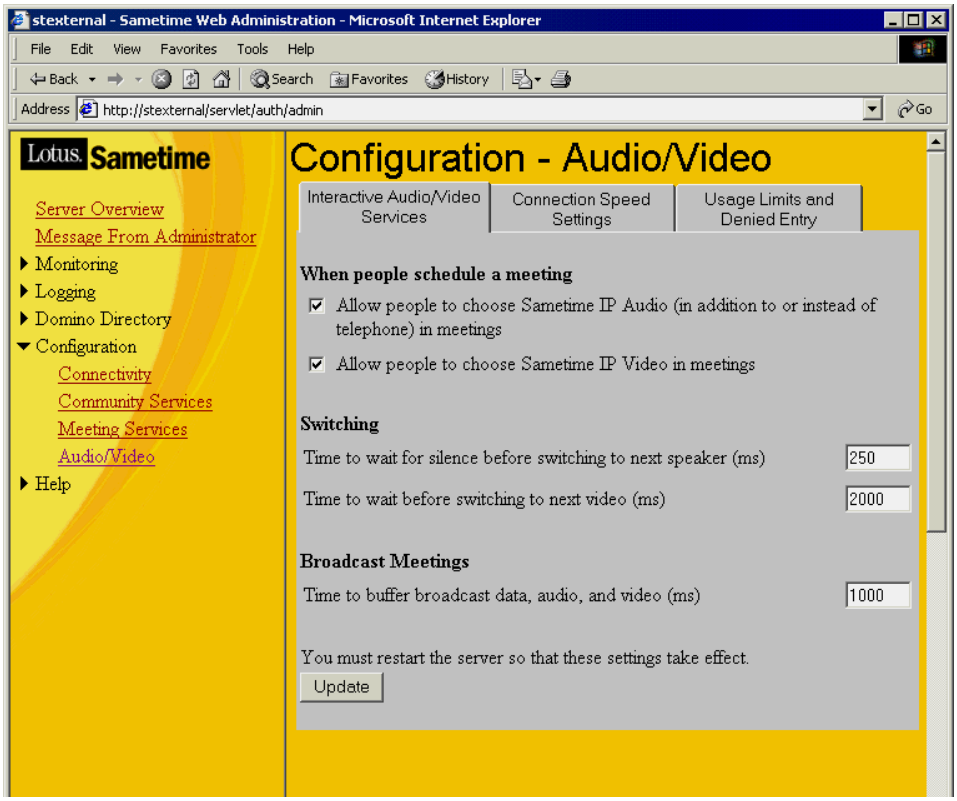


Figure 30. Initial audio/video configuration screen of the administration client

4. Click on the Connection Speed Settings tab. You should now see the screen in Figure 31.

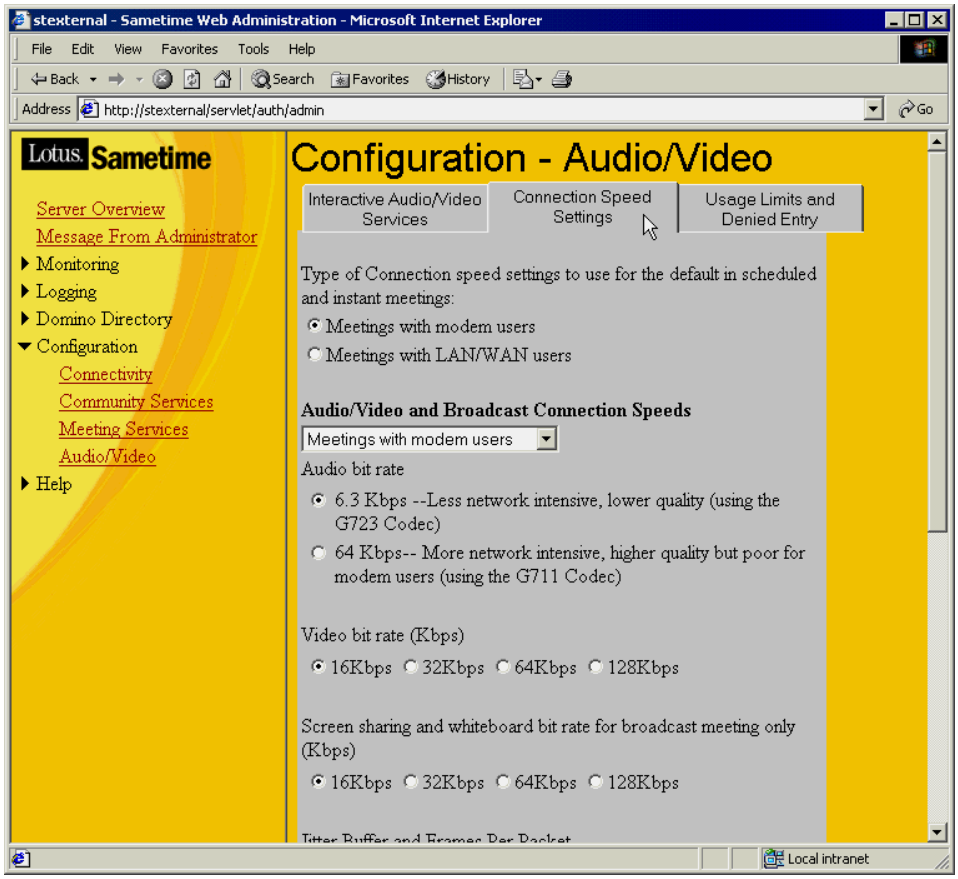


Figure 31. Connection speed settings tab

5. From the drop-down specify the connection type you would like to modify the Jitter buffer for; that is, either modem users or LAN users.

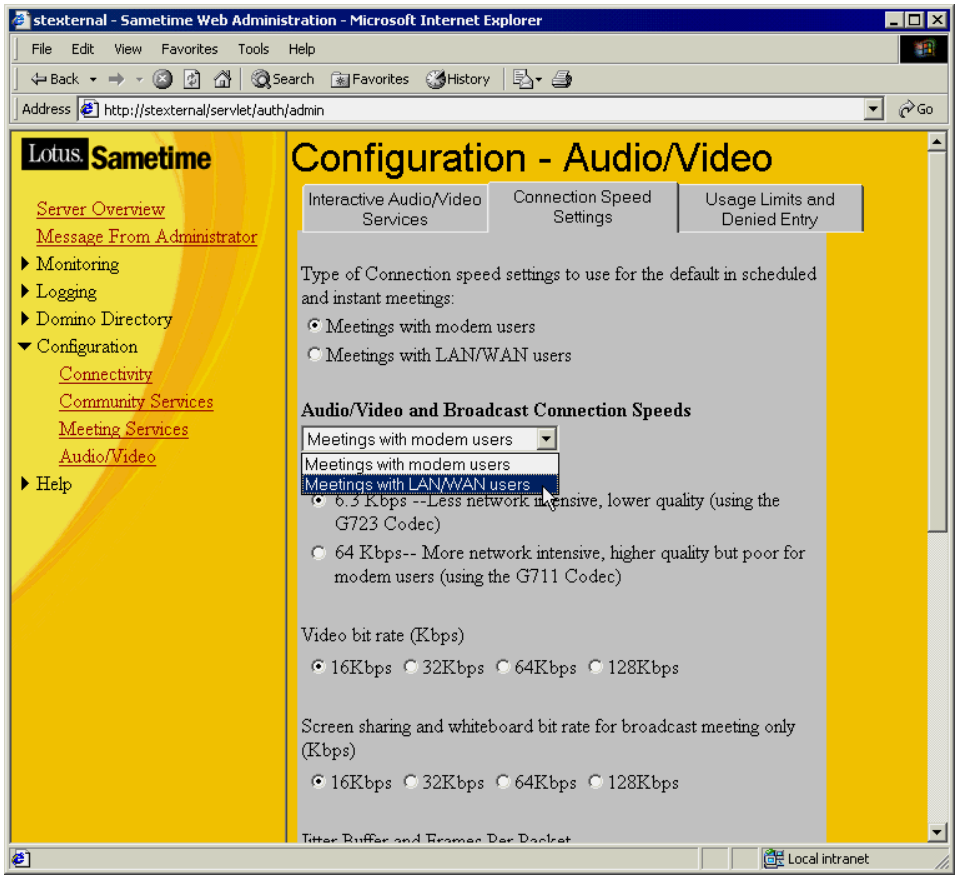


Figure 32. Choosing the connection type

6. Once you have chosen a connection type, scroll down the page and enter the number of milliseconds you wish to buffer. Refer to Figure 33 on page 76.

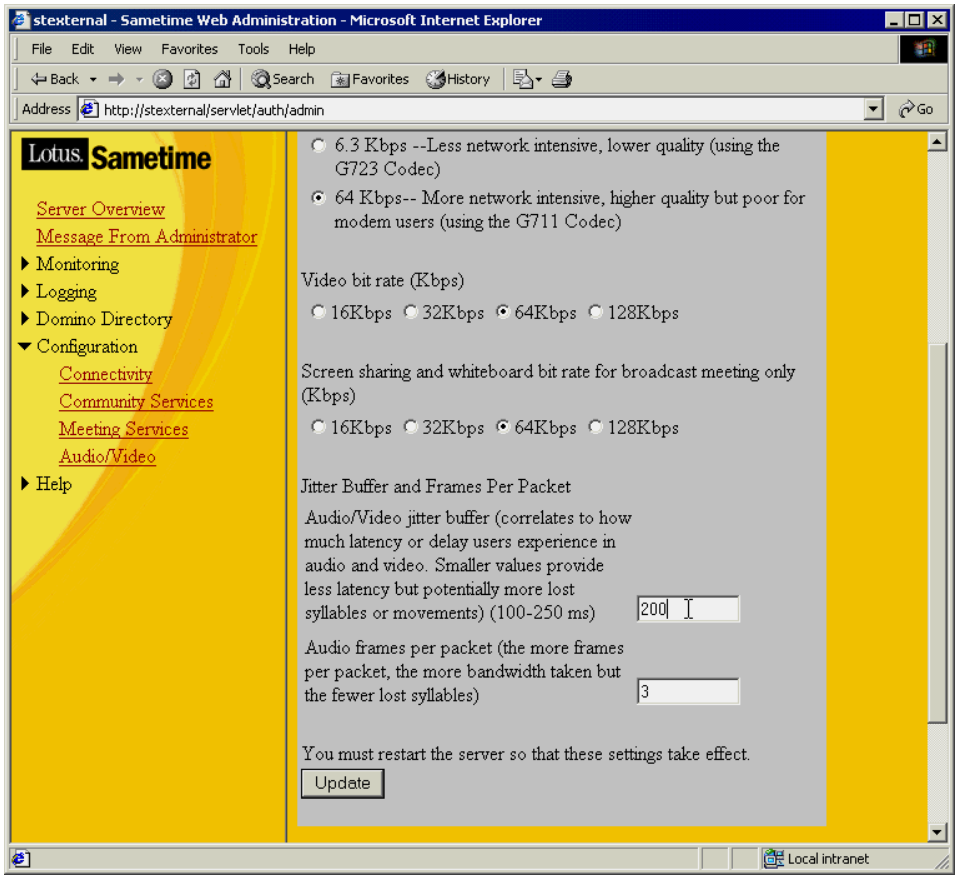


Figure 33. Specifying the jitter buffer

7. Click the Update button and restart the server for the change to take effect.

3.3.4 Usage limits and denied entry

Sametime provides the administrator with the ability to limit the amount of video. Unlike Sametime 1.5, the limits in Sametime 2.0 are hard limits: once they have been reached, a user will receive a message informing them that the limit has been reached and that they cannot connect to the meeting. (At the time of writing this doesn't appear to be working correctly in Sametime 2.0 beta 2.)

A Sametime administrator can limit the number of audio and video connections for instant meetings, scheduled meetings, and broadcast

meetings. This facility has been provided in Sametime to prevent the network from becoming overloaded. An overloaded network will result in poor quality audio and video.

Following is an example of how to limit the number of audio and video connections for instant meetings.

1. Open the Sametime administration client by clicking on the “Administer the server” link on the Sametime meeting center homepage.
2. A new browser window containing the administration client will be launched.
3. Expand the Configuration link and select Audio/Video. You should now see a screen like Figure 34.

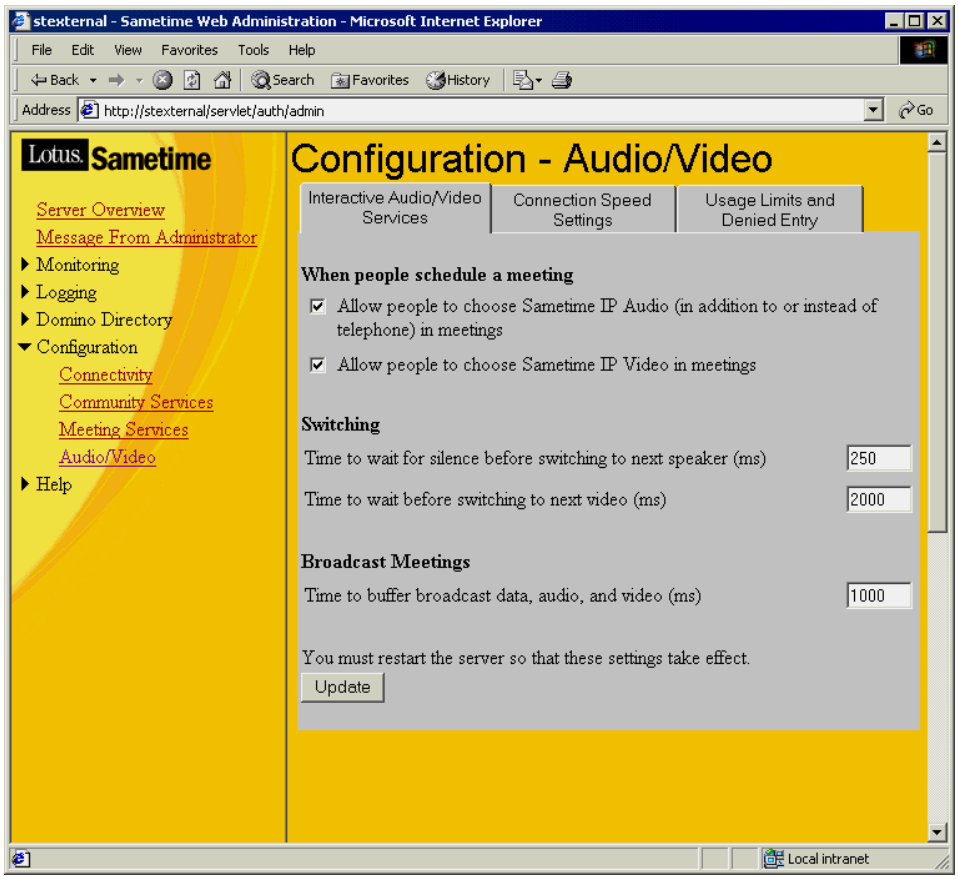


Figure 34. Initial audio/video configuration screen of the administration client

4. Click on the Usage Limits and Denied Entry tab. You should now see the screen shown in Figure 35.

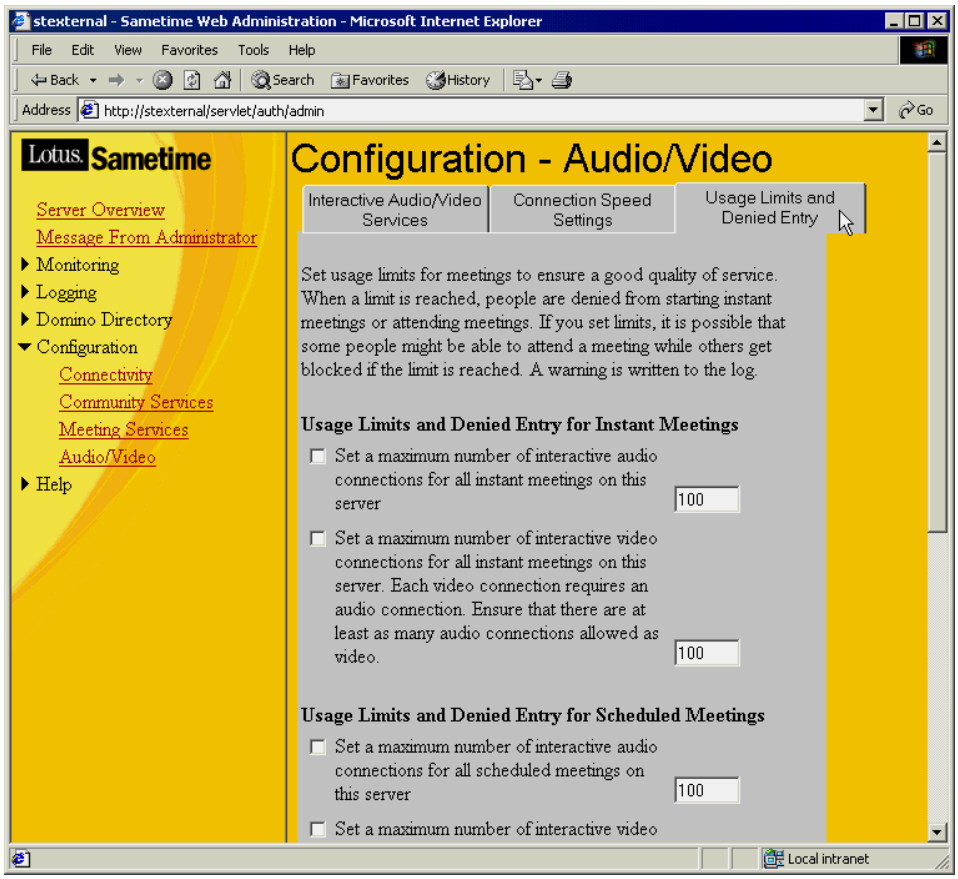


Figure 35. Usage Limits and Denied Entry tab

5. Check the first two checkboxes. The first checkbox will limit the number of audio connections to the value specified in the field. The second checkbox will limit the number of video connections to the value specified in the field.
6. If you limit any audio or video connection, be sure to limit *both* streams to the same number. That is, if you want to allow only 10 audio streams for instant meetings, you should also allow only 10 video streams for instant meetings.

3.4 Summary

This chapter has provided information on the various audio and video codecs utilized by Sametime 2.0. We have provided information on how to estimate bandwidth for each codec based on the audio frames per packet setting. We have also shown the effect the audio frames per packet setting has on network bandwidth utilization. Example calculations to aid you in calculating bandwidth utilization in your organization have been provided.

Finally, we have described various audio/video settings that are configurable via the Sametime administration client and provided detailed instructions for how to configure these settings.

Chapter 4. Under the covers of Sametime

Sametime consists of client and server applications that enable a community of users to collaborate in real time over any TCP/IP network.

This chapter describe the various components of both Sametime servers and clients. Understanding their individual roles helps a Sametime architect to make better decisions when planning for a Sametime infrastructure. In case of system problems, it can also assist an administrator in troubleshooting.

In addition to a detailed explanation of the Sametime core architecture, we are also going to cover tips and tricks with regard to security and single signon solutions.

Finally, we provide some real world examples of extensions to a Sametime infrastructure, including multi-language translation capabilities and support for mobile Sametime users.

4.1 Sametime server components

This section describes the different services of a Sametime 2.0 server.

A Sametime server consists of the following modules:

- Community Services
- Meeting Services
- Multimedia Services
- Broadcast Services
- Domino DNA

Community Services, Meeting Services and Multimedia Services can be used in scheduled as well as in instant online meetings.

The following sections explain the role of each of these components in greater detail.

4.1.1 Community Services

The Sametime Community Services support all presence (or awareness) and text chat activity in a Sametime community. Any Sametime client that contains a presence list (for example, the buddy list in Sametime Connect) must connect to the Community Services. The Community Services clients include the Sametime Connect client, the Sametime Meeting Room client with the

Participant List and meeting chat components, and presence lists in Sametime Discussion or TeamRoom databases. Sametime Community Services provide clients with the ability to see each other's online status (= awareness), communicate in instant messaging sessions, and participate in group chats.

Basic functionality supported by the Community Services includes:

- Handling client login requests
- Handling connections from clients that access the Sametime server through a direct TCP/IP connection, HTTP, HTTPS, or SOCKS proxy servers
- Providing directory access for user name search and display purposes
- Providing directory access to compile lists of all Sametime servers and users in the community
- Dissemination of presence and chat data to all users connected to Community Services
- Maintenance of privacy information for online users
- Interacting with the Meeting Services to create meetings in which collaborative activities supported by the Community Services, Meeting Services, and Audio/Video Services (if installed) are simultaneously available
- Handling connections from the Community Services on other Sametime servers when multiple servers are installed
- Logging of Community Services events to the Sametime log (STLOG.NSF)

Figure 36 on page 83 shows the major components of Community Services together with their main clients.

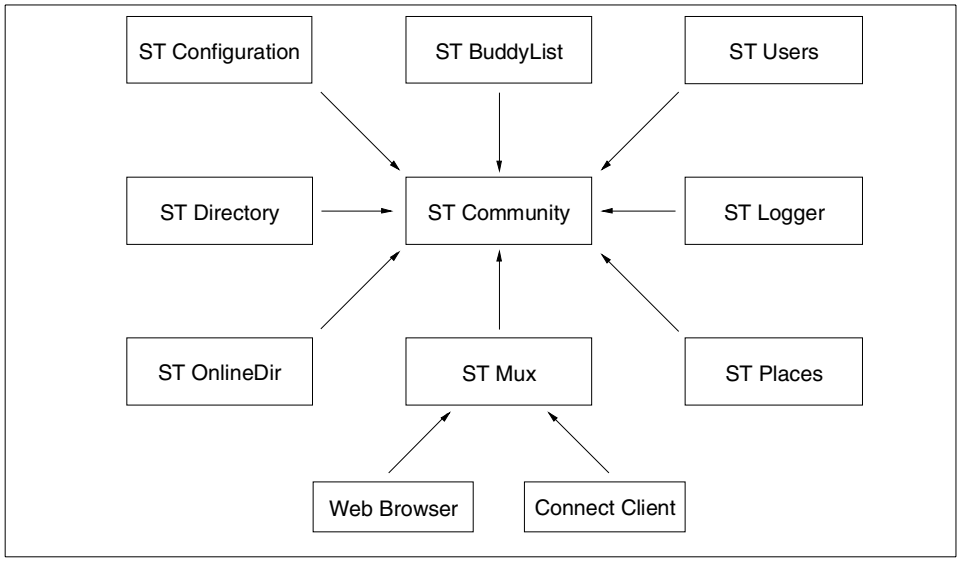


Figure 36. Community Services components

The roles of these components are as follows:

- **ST Community Launch** is responsible for starting up and shutting down all other Community Service components, as well as keeping them alive.
- **ST Community** acts like a switchboard for all other Community Services tasks. It manages channels and messages between other Community Services clients and server components. ST Community plays an important role in authentication, encryption and distribution.
- **ST BuddyList** provides the "Who Is Online" service. This component keeps track of who logged in and out. Clients send their presence or awareness list to this component and are notified of status changes. This component takes into account privacy information, status, and who is interested in this user. ST BuddyList is also responsible for maintaining and pushing values of different community attributes, which are controlling the client behavior (for example, services that are enabled/disabled in the server).
- **ST Conference** provides for multi-user chat and Who Is Here (WIH) services. Each conference takes place in a "place" and has a list of participants.
- **ST Configuration** periodically reads the server configuration from the Sametime directory. It also stores and retrieves information about the user

preferences and retrieves and pushes community attributes to the ST Buddy List service.

- **ST Directory** provides directory access and browsing capabilities against the Sametime directory. It also allows users to get the content of a public group.
- **ST Logger** is responsible for logging various events to a text file and/or a Notes database.
- **ST Mux** handles the communication load. Clients connect to the multiplexer rather than directly to the server. The multiplexers maintain a TCP/IP connection to the server. By default there's one multiplexer per server.
- **ST OnlineDir** holds a status snapshot of the community (who is online, number of logins per person). In addition, it has two primary roles: handling preferred logins and enforcing login.
- **ST Places** creates and maintains information about places in the Sametime community. A "place" is an instrument, where conferences and meetings are being held (both instant and scheduled meetings). The ST Places component stores the state and properties of each place, including the list of people currently in the place.
- **ST Users** handles all authentication requests. It also handles all search requests (resolve) to return a unique User ID for each entry that is found in a search reques, and all privacy information requests (set and get).

A Sametime Administrator can see most of the Community Services components running as Windows services on the Sametime server machine. Figure 37 on page 85 shows Sametime Community Services running on a Windows 2000 system.

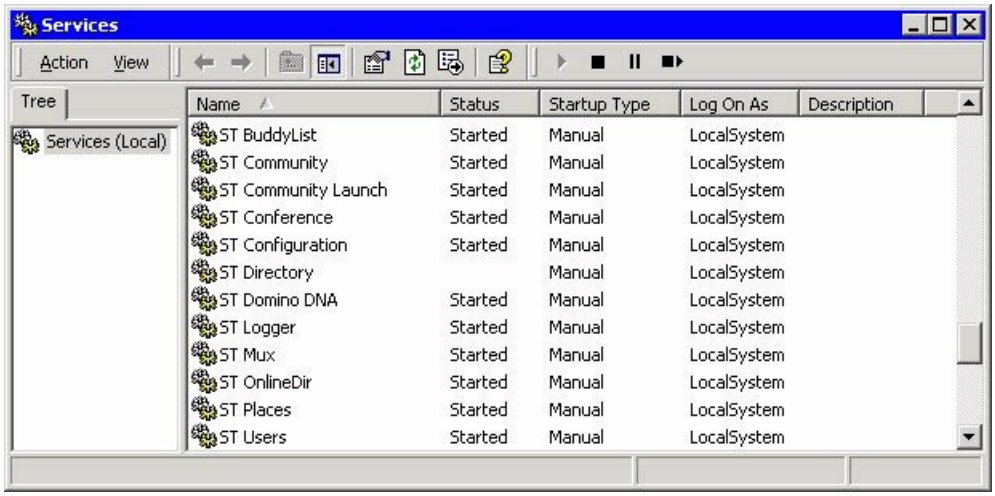


Figure 37. Windows 2000 Services control panel showing Community Services components

Community Services also provide for the persistent storage of user properties. Among these properties are user preferences, buddy list, and privacy information; as well as information about the availability of audio and video hardware on the user's PC. This information is stored in the database vpuserinfo.nsf on a user's home Sametime server.

4.1.2 Meeting services

Meeting services provide a shared whiteboard, which can be pre-loaded with presentation files, diagrams, word processing documents, and so forth, for scheduled meetings. They also offer screen sharing, which allows remote users to see and optionally control applications running on a host computer (= the application sharing host) without the need to install the application on the local system. Meeting services are also responsible for starting, stopping and deletion of meetings.

The main component of Meeting Services is a T.120 multipoint communications unit (MCU), which supports the Sametime Meeting Room client (MRC) as well as other T.120-based clients like Microsoft NetMeeting. If the Sametime Multimedia Services add-on is installed on the server, Meeting Services also support connections for the interactive audio/video components of the Sametime Meeting Room client.

Basic functionality of the Meeting Services includes:

- Creating and destroying meeting objects.

- Handling connections from clients that access the Sametime server through a direct TCP/IP connection, or through HTTP, or SOCKS proxy servers.
- Dissemination of T.120 screen-sharing and whiteboard data among multiple users in a meeting.
- Maintaining lists of active, scheduled, and completed meetings.
- Starting and stopping instant and scheduled meetings at the appropriate times.
- Interacting with the Community Services to create meetings in which collaborative activities supported by the Community Services, Meeting Services, and Audio/Video Services (if installed) are simultaneously available.
- Allowing the administrator to control which collaborative activities are available to end users of the Sametime server.
- Handling connections from the Meeting Services of other Sametime servers when a community includes multiple Sametime servers. These connections enable a single meeting to be active on multiple Sametime servers.
- Logging Meeting Services events to the Sametime log (STLOG.NSF).

4.1.3 Multimedia services

If the Multimedia add-on is installed on a Sametime server, Sametime 2.0 provides for interactive multipoint audio/video conferencing and the ability to broadcast audio/video/data presentations over any TCP/IP network, including entire corporate networks and the Internet. Note that data conferences will work without the multimedia services being installed.

The Multimedia add-on consists of 3 main elements:

- Multimedia Multipoint Control Unit (MMCU)
- Multimedia Processor (MMP)
- Broadcast Gateway

The Multimedia Multipoint Control Unit and the Multimedia Processor allow users via the Sametime Meeting Room Client (MRC) or any other H.323 endpoint (for example Microsoft NetMeeting) to participate in interactive audio/video meetings.

4.1.3.1 Multimedia Multipoint Control Unit

The Multimedia Multipoint Control Unit (MMCU) manages the audio/video call setup and control between the client and server. When a client establishes a connection to a Sametime 2.0 server in order to participate in a meeting, the MMCU passes a list of meeting attributes to the client including:

- Audio codec in use (G.711 or G.723)
- Video codec in use (H.263+, only if video is present)
- Video bit rate (16Kbps to 128Kbps, only if video is present)
- Encryption is enabled/disabled (not available for NetMeeting, only for MRC)
- UDP ports and TCP tunneling ports for audio and video streams

The MMCU also interacts with the Multimedia Processor (MMP) to set up the call and coordinate the video source with the audio source.

4.1.3.2 Multimedia Processor

The Multimedia Processor (MMP) manages the audio and video Real Time Protocol (RTP) streams. It controls the distribution of the audio and video streams to all clients in the meeting. The MMP scans all meeting participants, who are connected to the MMCU. When a meeting participant speaks, the MMP locks onto that client's audio stream and distributes that stream to all other clients in the meeting. When a participant stops speaking, the MMP waits for a brief period of time (the "Time to wait for silence before switching to next speaker"), and then begins to scan for other active audio clients. This time interval prevents the MMP from switching during normal pauses in conversation, because rapid audio switching would place unnecessary load on the system CPU and consume network bandwidth.

Each time the MMP switches to a new audio source, it sends an event to the MMCU. The MMCU, through its connections to the clients, ensures that an icon indicating the current speaker is updated for all clients. After this update, the MMCU instructs the MMP to set the video source to the person currently speaking.

To prevent video from switching too rapidly (which would reduce usability and consume considerable network bandwidth), the administrator can control the time interval that must pass before the video switches to the next person. This time interval is specified as the "Time to wait before switching to the next video (ms)".

If the current speaker does not have video capabilities or has the video window paused, the MMCU ensures that all client "Speaker's Video" windows are also paused.

The MMP can lock onto and broadcast a maximum of two audio streams at the same time. In a Sametime meeting, if two people speak at the same time, it is possible for all meeting participants to simultaneously hear both people speaking. However, if three people speak simultaneously, only two of the people will be heard. The MMP designates the audio stream that has been transmitting the longest (generally the person, who started speaking first) as the primary audio stream. The source of the primary audio stream is also the source of the video stream.

As different people speak during a meeting, the MMP performs switching operations in either automatic microphone mode (= default setting for all Sametime audio meetings) or request microphone mode. Full-duplex sound cards are required to participate in either automatic microphone or request microphone mode.

4.1.3.3 Automatic microphone mode

In *automatic microphone* mode, as one meeting participant begins to speak, the MMP will lock onto that audio stream and output it to all the other clients in the meeting automatically. If another participant also begins to speak, the MMP will lock onto that audio stream as well. The two audio streams are sent to all other participants and mixing occurs at the client. In the case of the two active speakers, their audio stream is sent to the other speaker. If a third participant begans speaking, the server would ignore that audio stream until one of the other active participants stopped speaking.

4.1.3.4 Request microphone mode

In *request microphone* mode only one participant is permitted to speak at a time. The user must request the microphone first. If the microphone is already in use by another participant, the requesting user is put into a queue. As additional users request the microphone, they are also put into the queue. As soon as the current active speaker releases the microphone, the first participant in the queue is granted access to the microphone.

The request microphone mode allows for a very controlled meeting where only one person speaks at a time (for example during presentations).

The queuing mechanism gives other attendees an opportunity to ask questions without interrupting the active speaker. It also provides feedback to an active speaker by showing a raised hand for the participant who wants to ask a question. The active speaker can then release the microphone.

Some H.323-compliant clients, such as Microsoft NetMeeting, can receive only one audio stream. These users will hear only one person speaking at a time (that is, they will receive only the primary audio stream).

H.323 clients also can't actively request the microphone. In Request Microphone mode, these clients are restricted to receiving audio and video only.

4.1.4 Broadcast services

In addition to these interactive collaboration tools, Sametime also provides Broadcast Services, which allows a large number of receive-only clients to participate in online meetings. Using streaming protocols, a broadcast meeting can scale up to several thousand meeting participants.

Basic functionality supported by the Broadcast Services includes:

- Handling connections from the Sametime Broadcast clients using the Real Time Streaming Protocol (RTSP)
- Handling connections from clients that access the Sametime server through a direct TCP/IP connection, or through HTTP or SOCKS proxy servers
- Negotiating with the Broadcast clients to ensure the clients can receive the meeting streams
- Identifying and attaching to broadcast meetings on the Sametime server
- Transcoding T.120 screen sharing and whiteboard data into RTP streams
- Transmission of screen sharing and whiteboard, as well as audio and video RTP streams, using User Datagram Protocol (UDP), TCP, or HTTP to ensure clients operating in a variety of different network environments can receive the streams
- Multicasting of data streams when transmitting on multicast-enabled networks
- Simultaneously broadcasting multiple meetings

The two server components that provide the Broadcast Services are:

- Broadcast Gateway Controller
- Broadcast Gateway

Generally, the broadcast gateway controller interacts with the Meeting Services on the Sametime server and passes control information to the broadcast gateway. The broadcast gateway handles client connections. It also

converts screen sharing, whiteboard, and audio/video data (if available) and transmits RTP streams containing this data to the Sametime Broadcast clients.

Figure 38 shows the broadcast gateway architecture.

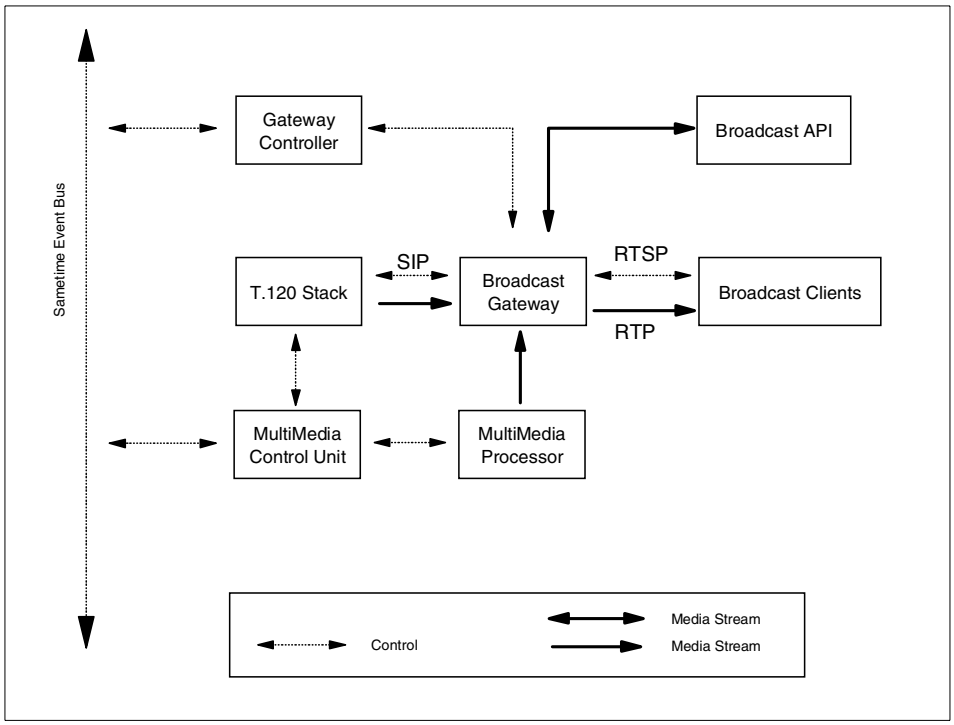


Figure 38. Broadcast gateway architecture

The Sametime broadcast architecture also allows you to publish and subscribe to media streams. This function is available through an API and allows for integration with other products using streaming protocols. For example, one could think of extensions built to deliver record and replay capabilities for Sametime meetings.

4.1.4.1 Broadcast gateway controller

The broadcast gateway controller is a Java application that resides on the Sametime server. Whenever a broadcast meeting becomes active, the broadcast gateway controller receives notification and meeting details through the Sametime event system. It then sends a command to the broadcast gateway, telling it to join the conference and make the broadcast streams available to broadcast clients. The command to join the meeting is

sent over a control connection that the broadcast gateway controller establishes with the broadcast gateway. This connection occurs over the "Broadcast gateway control port" (default TCP port 8083) specified in the broadcast services Network and Port settings of the Sametime Administration Tool.

When a meeting is terminated, the gateway controller checks to see if the meeting is active on the broadcast gateway. If so, it sends a command to leave the meeting.

4.1.4.2 Broadcast gateway

When the broadcast gateway joins a meeting, it connects to the Sametime Meeting Services (T.120 server) in order to:

- Gain access to the screen sharing and whiteboard data exchanged during the meeting
- Transcode the application-sharing or whiteboard data into an RTP stream
- Transmit the RTP stream to the Broadcast clients

This connection takes place on the “Meeting server port for client connections” (default port 8081). To set this port, go to the Sametime Administration Tool and select Configuration -> Connectivity -> Networks and Ports. The port can then be found in the Meeting Services Network section as shown in Figure 39 on page 92.

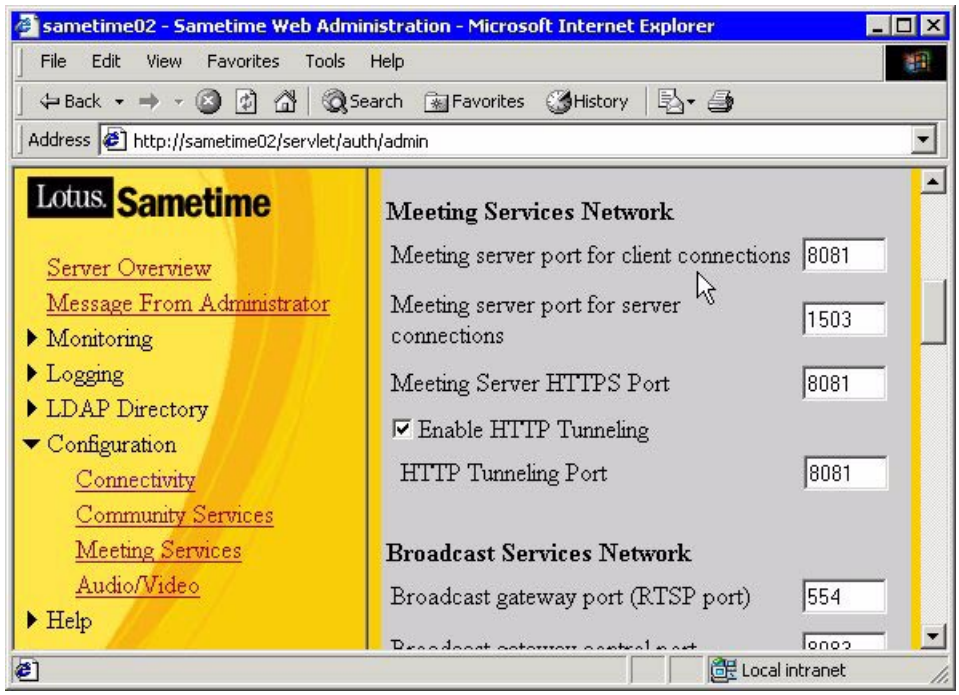


Figure 39. Meeting services network settings

If the Sametime Multimedia Services add-on is installed, the broadcast gateway can communicate with the MMCU through a T.120 channel using the IETF Session Initiation Protocol (SIP) to access the audio and video streams handled by the MMP. The broadcast gateway exchanges control messages with the clients using the Real Time Streaming Protocol (RTSP). It transmits all media streams to the Broadcast clients using the Real Time Protocol (RTP).

RTP can make use of either the UDP transport (for unicast or multicast), or tunnel the streams through a TCP/IP connection, a SOCKS 4 proxy server, or an HTTP proxy server. If multicast is enabled for the meeting, the gateway broadcasts each stream on a different multicast address. Sametime Broadcast clients learn about multicast addresses in use via RTSP.

The Sametime administrator can define values for the "Audio bit rate", "Video bit rate" and "Screen sharing and whiteboard bit rate" to control the rate at which the audio, video and data (screen sharing and whiteboard) streams are transmitted to the clients.

To define these settings, go to Configuration -> Audio/Video -> Connection Speed Settings in the Sametime Administration Tool. The bit rates can then be set in the Audio/Video and Broadcast Connection Speeds section.

Figure 40 shows the connection speed settings for audio/video and broadcast services.

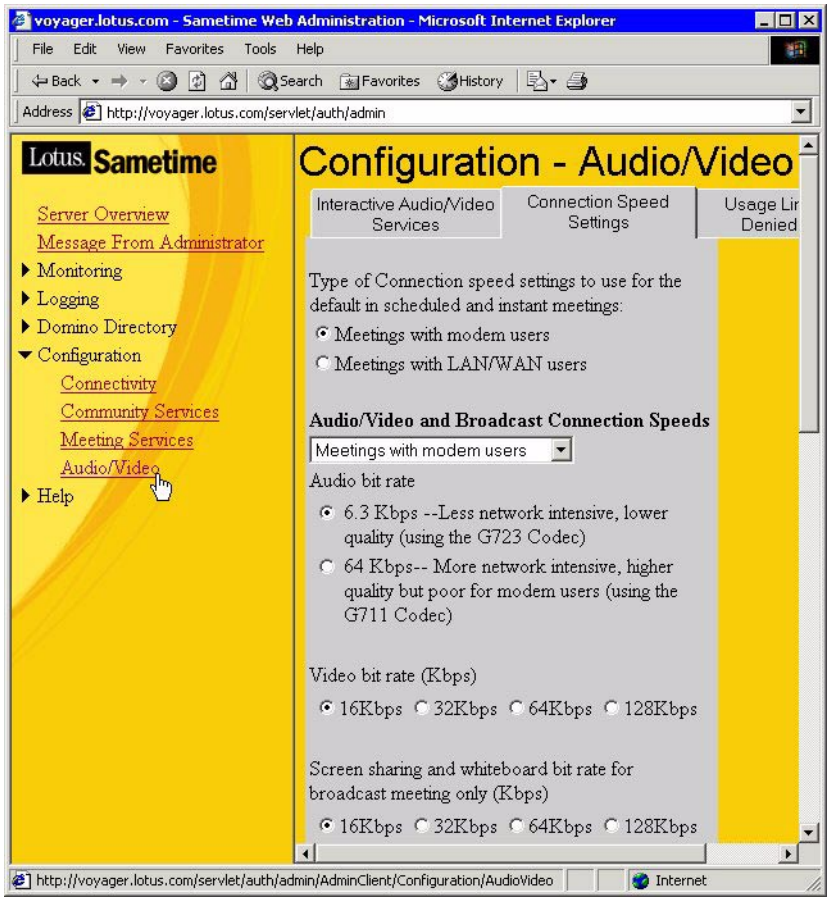


Figure 40. Connection speed settings for audio/video and broadcast services

The broadcast gateway can participate in multiple meetings at the same time. The maximum number of meetings and the maximum number of clients both depend on how much transcoding is going on in each meeting and what transports are being used for each client. At the time of this writing, however, there is no scalability information about the broadcast gateway available. For more recent information check the following Web sites:

`http://www.lotus.com/sametime and http://stdev.lotus.com`

Note: For scalability reasons, the broadcast gateway can be run on a separate machine. For more information see 2.4.2, “Multiple Sametime servers” on page 33.

For more information on the audio/video attributes and the transmission of Broadcast streams to the Broadcast clients, see the topics "Connection Speed Settings for Audio/Video Services" and "Broadcast client connection process" in the Sametime 2.0 Administrator's Guide.

4.1.5 Domino DNA

Depending on the type of installation, a Sametime server includes either a full Domino server (when installed on top of an existing Domino server) or a reduced set of core Domino modules called Domino DNA (when installed as a Web-only server or as another server within an existing Domino domain). In either case, core Domino capabilities like directory, security, mail routing, replication and Web application services are available. The architecture of Lotus Domino is beyond the scope of this book. For a detailed explanation see the following publication, which describes the internal architecture of Notes and Domino in sufficient detail to enable you to make optimal deployment and programming decisions:

Inside Notes: The Architecture of Notes and the Domino Server, available at:

`http://www.notes.net/notesua.nsf/find/inside-notes`

4.2 Sametime Clients

This section describes the different client options and their specific behaviors when connecting to the Sametime server. When planning for a Sametime 2.0 infrastructure, it's important to understand the deployment requirements for the individual clients as well as the details of the client connection process.

There are several Sametime clients, each of which makes use of the Sametime services (Community Services, Meeting Services, Multimedia Services, Broadcast Services) in different ways. The most common clients are Sametime Connect, the Sametime Meeting Room Client, and the Sametime Broadcast Client. Besides that, any Sametime-enabled application acts as a client talking to a Sametime server. The Discussion and TeamRoom databases in Sametime 2.0, as well as the "Who is online" feature in the Notesmail application as of Notes 5.0.2 and higher, are examples of Sametime-enabled applications.

4.2.1 The home Sametime server

Sametime incorporates the concept of a *home* Sametime server. In an environment with multiple Sametime servers or in case of Sametime-enabled databases running on other Domino servers within the community (as is the case when using the "Who is online" feature in Notesmail 5.0.2 and above), a home Sametime server must be defined in a user's person record either in the Sametime directory or in the LDAP directory. As mentioned in the section about Community Services, it is the user's home Sametime server that provides for the persistent storage of user properties like preferences, buddy lists, and privacy information; as well as information about the availability of audio and video hardware on the user's PC. This information is stored in the database vpuserinfo.nsf on the user's home Sametime server. Because of this, the home Sametime server plays an important role in the process of a client connecting to a Sametime community.

The Sametime Connect client and the Sametime Meeting Room client both connect to Community Services on the Sametime server.

This connection process and login to the Sametime community takes place in two phases:

1. The connection phase: The Sametime Connect client creates a TCP/IP connection to the Sametime server, which is specified in the Sametime Connect client's connectivity settings. Details about this connection process are described later in this chapter. In the case of the Meeting Room client this connection is made back to the Sametime server, on which the client attended the meeting.
2. The login phase: The client's request to log in to the community is transferred to the client's home Sametime server. The home Sametime server authenticates the client against the community directory and verifies that the user is authorized to enter the community. Regarding the underlying network connections, it's actually the Sametime server from the connection phase in step 1 (and not the client) which connects to the home Sametime server to transfer the user's login request.

Usually the server the user connects to in the first phase will be the same as the home Sametime server, although technically this is not required. It is, however, recommended to directly connect to the home Sametime server, because this is usually more efficient than using the internal redirection process described above. To achieve this, the settings for a user's home Sametime server (in his/her person record in the Sametime directory) must correspond to the name of the Sametime server specified in the Connect client. Note that the settings in the Sametime Connect client specifies the

server name with its DNS name or IP address, whereas the value in the "Sametime server" field in a user's person record specifies the fully hierarchical Sametime (or Domino) server name.

In the example shown in Table 16, there are two Sametime servers available: Server1 and Server2.

Table 16. Sametime server naming schema

Machine	DNS name	Sametime (or Domino) server name
Server1	stserver1.acme.com	CN=stserver1/OU=Servers/O=ACMECorp
Server2	stserver2.acme.com	CN=stserver1/OU=Servers/O=ACMECorp

Case A - The settings in the Sametime Connect client and in the “Sametime server” field in the user’s person record don't match:

Sametime Connect client: stserver1.acme.com

“Sametime server” field: CN=stserver2/OU=Servers/O=ACMECorp

In this case, the Sametime Connect client connects to Server1 first and is then redirected to it's home server, Server2. This configuration is less efficient than case B.

Case B - The settings in the Sametime Connect client and in the “Sametime server” field in the user’s person record match:

Sametime Connect client: stserver1.acme.com

"Sametime server" field: CN=stserver1/OU=Servers/O=ACMECorp

This is the recommended case. Since both settings specify the same server (=Server1), the client connects directly to the home Sametime server.

There are, however, exceptions to this recommendation. While in a remote office, a travelling user might want to simply connect to the nearest available Sametime server. Or a company might want to set up a Sametime server that is accessible over the internet. This server could be used for the initial client connection and could redirect login requests to the user's internal home Sametime server, which of course is not directly accessible over the firewall. More details about such a configuration is in the section about the demo scenario. In any case, the user will always be authenticated by their home Sametime server, because all user preferences, buddy lists, and privacy information is stored only on the home Sametime server.

4.2.2 Sametime Connect client

Sametime Connect is a Windows 32 application, written in C++, that runs on a user's local computer. It provides online awareness within presence lists (also known as buddy lists), directory browsing, privacy features, and instant messaging, as well as group chat capabilities. It also allows the user to initiate instant meetings between two or more users by launching the Sametime Meeting Room client. Sametime Connect also interoperates with America Online's Instant Messenger (AIM). Connect users can add AIM users to their buddy list to see if they're online and chat with them just as with any other Sametime user. It is not possible, however, to have a common chat session between multiple Sametime and AIM users. Only individual instant messaging conversations between a Sametime Connect client and AIM users are supported.

4.2.2.1 Sametime Connect client connection process

The Sametime Connect client connects to Community Services on the Sametime server. The Community Services on the Sametime server listen for direct TCP/IP connections from the Sametime Connect client on the "Community server port for client connections" (port 1533 by default). This port is not configurable. Community Services also support connections from clients coming in via HTTP, HTTPS, or SOCKS proxy servers. Select Configuration -> Connectivity -> Network and Ports in the Sametime Admin Tool to specify the Community Services Network settings as shown in Figure 41.

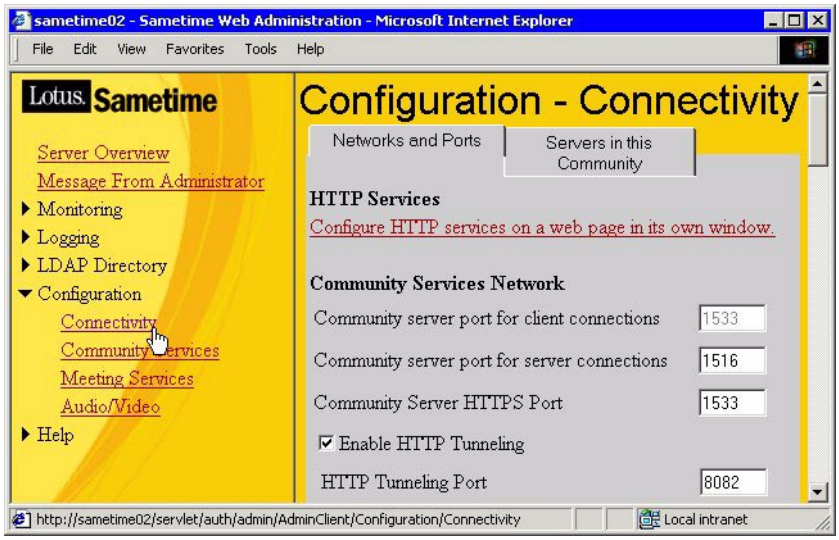


Figure 41. Connectivity settings for Community Services in Sametime Admin Tool

In an Intranet environment, Sametime Connect would normally use a direct TCP/IP connection on port 1533. It can also connect through a SOCKS, HTTP or HTTPS proxy server. In either case, the connectivity settings specified in the Sametime Connect client must match the corresponding connectivity settings on the Sametime server. To specify the connectivity settings in the Sametime Connect client go to Options -> Preferences -> Sametime Connectivity.

Figure 42 shows the Sametime Connectivity settings in the Sametime Connect client. In this specific example, the Sametime Connect client is configured to connect to the Sametime server (stserver1.meetings.com) via Acme's http proxy (webproxy.acme.com). In this case, the Sametime server must listen for incoming http connections on the "HTTP Tunneling Port" 8082 (this is discussed in more detail in the next secton).

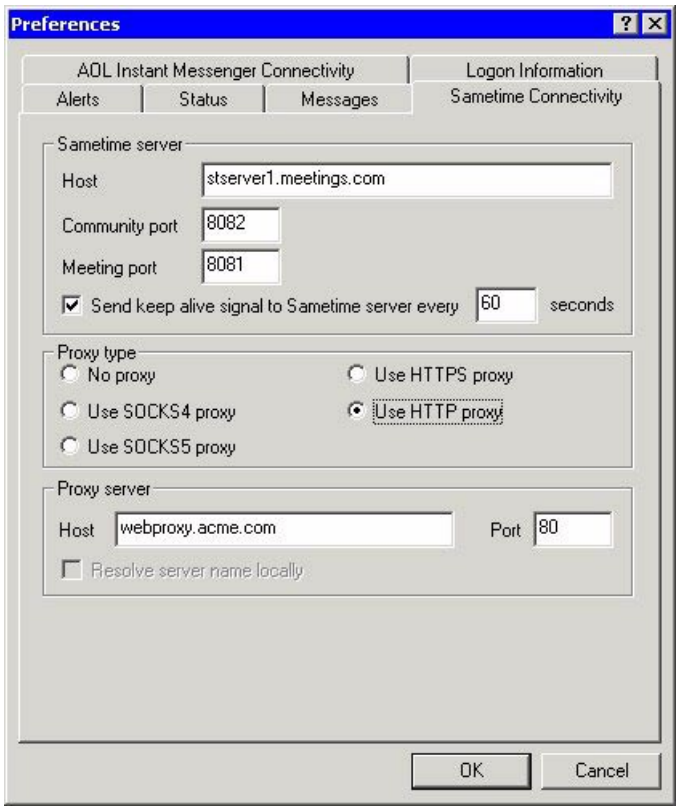


Figure 42. Sametime Connectivity settings in Sametime Connect client

The Sametime Connect client's connection process occurs as follows:

1. The user opens the Sametime Connect client.
2. The Sametime Connect client connects to the Sametime server specified in the “Host” field of the Sametime Connect client's Sametime Connectivity settings. The “Proxy type” setting controls how the connection occurs:

No proxy: If *No proxy* is selected, Sametime Connect attempts a direct TCP/IP connection on the “Community port” (default port 1533). The “Community port” setting in the Sametime Connect client must match the “Community server port for client connections” setting on the Sametime server. If the client needs to cross a firewall to access the Sametime server and the firewall blocks TCP port 1533, a direct connection cannot be established.

SOCKS proxy: If the Sametime Connect client has to go through a *SOCKS proxy* to connect to a Sametime server, the user must specify the Host name (DNS name or IP address) of the SOCKS proxy server and the port to connect to it. In the case of a SOCKS5 proxy, the user can also enter a user name and password required for SOCKS5 authentication. The “Community port” setting in the Sametime Connect client must match the “Community server port for client connections” setting on the Sametime server. The SOCKS proxy connects to Community Services on the Sametime server on behalf of the client. The Community Services listen for this connection on port 1533. If the SOCKS proxy needs to cross a firewall to access the Sametime server, this port must be open on the firewall.

Use HTTPS proxy: Choose this setting if the Sametime Connect client connects to an HTTPS proxy in order to access a Sametime server. You also have to specify the Host name (DNS name or IP address) of the HTTPS proxy server and the port required to connect to it. By default the Sametime client attempts to talk to the HTTPS proxy on port 443. If the HTTPS proxy requires authentication, a user name and password can be specified.

In this configuration the “Community port” setting in the Sametime Connect client tells the HTTPS proxy server on which port it should connect to Community Services. It must match the “Community server HTTPS port” setting on the Sametime server. The HTTPS proxy connects to Community Services on the Sametime server on behalf of the Sametime Connect client. If the HTTPS proxy must cross a firewall to access the Sametime server, the “Community server HTTPS port” (port 1533 by default) must be open on the firewall. When connecting through an HTTPS proxy, no encryption is involved and the Sametime server does not need to recognize any other protocol besides it's normal protocol.

Use HTTP proxy: Choose this setting if the Sametime Connect client connects to an HTTP proxy in order to access a Sametime server. You also have to specify the Host name (DNS name or IP address) of the HTTP proxy server and the port required to connect to it.

In this configuration the “Community port” setting in the Sametime Connect client tells the HTTP proxy server on which port it should connect to Community Services. For this connection to succeed, “Enable HTTP Tunneling” must be activated on the Sametime server and the Sametime Server “Community port” specified in the Sametime Connect client must match the “HTTP Tunneling port” on the Sametime server. By default, both port settings are 8082.

The HTTP proxy connects to Community Services on the Sametime server on behalf of the Sametime Connect client. If the client or the HTTP proxy must cross a firewall to access the Sametime server, the “HTTP Tunneling port” (port 8082 by default) must be open on the firewall.

Note

To allow Internet clients to access a Sametime server, you can deploy the Sametime server outside of the firewall or use a multiple Sametime server configuration. For more information about making a Sametime server inside the firewall accessible to clients connecting over the Internet, see “Advantages of using multiple Sametime servers” in the Sametime 2.0 Administrator's Guide. For information about connecting through restrictive firewalls, see “Tunneling on port 80” in the Sametime 2.0 Administrator's Guide.

4.2.2.2 Connecting to the AOL Instant Messenger service

The Sametime Connect client can also connect to an America Online Instant Messenger server, allowing users to participate in chats with AOL Instant Messenger users. On the Internet, Sametime Connect would normally use a direct TCP/IP connection to the AOL Host (login.oscar.aol.com on port 5190). It can also connect through a SOCKS or HTTPS proxy server. To specify the connectivity settings for AOL in the Sametime Connect client, select Options -> Preferences -> AOL Instant Messenger Connectivity.

If the Sametime Connect client has to go through a *SOCKS proxy* to connect to the AIM service, the user must specify the Host name (DNS name or IP address) of the SOCKS proxy server and the port to connect to it. In case of a SOCKS5 proxy, the user can also enter a user name and password required for SOCKS5 authentication. The SOCKS proxy connects to the AIM service

on behalf of the Sametime Connect client. If the SOCKS proxy needs to cross a firewall to access the AOL server, TCP port 5190 (=the target port on the AOL Host) must be open.

Use HTTPS proxy: Choose this setting if the Sametime Connect client connects to an HTTPS proxy to access the AIM service. You also have to specify the Host name (DNS name or IP address) of the HTTPS proxy server and the port required to connect to it. By default the Sametime Connect client attempts to talk to the HTTPS proxy on port 443. If the HTTPS proxy requires authentication, a user name and password can be specified.

The HTTPS proxy connects to the AIM service on behalf of the Sametime Connect client. If the HTTPS proxy must cross a firewall to access the AOL server, TCP port 5190 (=the target port on the AOL Host) must be open on the firewall.

Users can also start instant meetings from the Sametime Connect client. Starting an instant meeting or responding to an instant meeting invitation launches a Web browser containing the Sametime Meeting Room client Java application. The Web browser and Sametime Meeting Room clients follow their own connection processes when connecting to the Sametime server to join instant meetings. For more information about the Sametime Meeting Room client, see the next section.

4.2.3 The Sametime Meeting center

The Sametime Meeting center is the main interface for Sametime clients to access meeting services. This application holds information about scheduled online meetings and whiteboard content. It is designed to be used by Web browsers only. However, since the information is stored in a Notes database (STConf.nsf), it is also possible to create and modify entries in the conferencing database programmatically by using common Notes and Domino application development tools like LotusScript. The Sametime Meeting Center allows users to create, modify and attend Sametime meetings.

4.2.4 Sametime Meeting Room Client

The Sametime Meeting Room Client (MRC) is a signed Java applet that runs in the Java Virtual Machine of the user's Web browser. It automatically downloads and installs to the local browser environment the first time a user enters a meeting. The MRC is cached on the user's machine to improve response time when attending subsequent meetings. It's updated automatically on the client whenever there's a new version available on the

Sametime server. Users participating in interactive online meetings will most often use the MRC since there's no need for manual deployment.

The Meeting Room client offers the following tools:

- Participants list
- Shared Whiteboard
- Screen Sharing
- Meeting Room Chat

In addition to these tools, if the Sametime Multimedia Services add-on is installed, the Meeting Room client also offers:

- A window to display and switch between the speaker's video and the user's local video
- Audio controls for microphone and speaker

During a meeting, various Java components contained within the MRC communicate with the Sametime server. These Java components use the initial connections established by the MRC to communicate with the different services on the Sametime server:

- **Participant List and Chat** - these components connect to the Community Services on the user's home Sametime server.
- **Screen Sharing and Whiteboard** - these components connect to Meeting Services.
- **Interactive Audio and Video** - connect to both Meeting Services and Audio/Video Services.

The server configuration and meeting type determines which of these tools are started automatically when a user enters a meeting. In any case, the Participants list will always be present.

4.2.4.1 Connecting to the Sametime server

Community Services provide virtual “places” that are used for n-way chat conferences and Sametime meetings. In the context of chat, you can think of a place like a chat room. For Sametime meetings, the place is an instrument that defines where the meeting is being held, or in other words, where the meeting “takes place.” The place holds different attributes that define the characteristics of the meeting. When the Sametime Meeting Room client launches, it connects to Community Services in order to access that meeting place. When the MRC is connected to the place, the participant list and the

meeting room chat components (if present) reuse the existing connection to Community Services.

4.2.4.2 Initial connection to Community Services

The MRC connects to the Community Services on the Sametime server as follows:

1. When a user attends a meeting, the Meeting Room client launches within the Web browser's Java Virtual Machine.
2. The port numbers on which the Community Services are listening for client connections are passed from the server to the client using HTML.
3. The MRC attempts a direct TCP/IP connection to the Sametime server on the “Community Server port for client connections” (port 1533).
4. If the direct TCP/IP connection fails, the MRC reads the Web browser's proxy settings. If they specify a SOCKS proxy, the TCP/IP connection to the “Community Server port for client connections” (port 1533) is routed through the SOCKS proxy. Only connections through SOCKS 4 proxy servers are supported. Connections through SOCKS 5 proxy servers are not supported, as a Web browser's Java Virtual Machine does not support SOCKS 5. The SOCKS proxy connects to the Community Services on the Sametime server on behalf of the MRC. The Community Services listen for this connection on port 1533. If the SOCKS proxy needs to cross a firewall to access the Sametime server, this port must be open.
5. If the connection attempt through the SOCKS proxy fails, or the Web browser's proxy settings do not specify a SOCKS proxy server, the client encases the connection information within an HTTP request and attempts an HTTP connection to Community Services. In this case, “Enable HTTP Tunneling” must be activated for Community Services on the Sametime server, so that the Community Services listens for HTTP connections on the “HTTP Tunneling port” (default port 8082).

If the Web browser's proxy settings specify an HTTP proxy, the client’s HTTP request is routed through the HTTP proxy, that is, the HTTP proxy server establishes the network connection to the Community Services on behalf of the MRC. If the MRC or the HTTP proxy must cross a firewall to access the Community Services on the Sametime server, the “HTTP Tunneling port” for Community Services (default port 8082) must be open on the firewall.

The Sametime Meeting Room client always attempts a direct TCP/IP connection to Community Services on port 1533 before examining the Web browser proxy settings or attempting an HTTP connection. A direct TCP/IP

connection results in better meeting performance than connecting through a proxy server or using the HTTP connection method.

4.2.4.3 Connecting to Meeting Services

After the MRC's initial connection to Community Services, the other meeting components (Screen Sharing, Whiteboard, Audio and Video) are started. They do not create new connections to the Community Server: they use the one already established by the MRC.

The Screen Sharing, Whiteboard, and Audio and Video components talk to Meeting Services. As with Community Services, there's no need for every component to establish individual connections to Meeting Services. Instead, the first component establishes a connection to Meeting Services, which is then reused by all remaining components as well.

The MRC connects to the Meeting Services on the Sametime server as follows:

1. As with Community Services, the port numbers on which the Meeting Services are listening for client connections are passed from the server to the client using HTML.
2. The MRC attempts a direct TCP/IP connection to the Sametime server on the “Meeting server port for client connections” (default port 8081). To prevent the Meeting Room client from attempting a direct TCP/IP connection, simply set the “Meeting server port for client connections” to zero (0). The MRC will then skip the direct TCP/IP connection attempt and directly read the Web browser's proxy settings.
3. If the direct TCP/IP connection fails, the MRC reads the Web browser’s proxy settings. If they specify a SOCKS proxy, the TCP/IP connection to the “Meeting server port for client connections” (default port 8081) is routed through the SOCKS proxy. Only connections through SOCKS 4 proxy servers are supported. Connections through SOCKS 5 proxy servers are not supported since a Web browser's Java Virtual Machine does not support SOCKS 5. The SOCKS proxy connects to the Meeting Services on the Sametime server on behalf of the MRC. The Meeting Services listen for this connection on the “Meeting server port for client connections” (default port 8081). If the SOCKS proxy needs to cross a firewall to access the Sametime server, this port must be open.
4. If the connection attempt through the SOCKS proxy fails, or the Web browser's proxy settings do not specify a SOCKS proxy server, the client encases the connection information within an HTTP request and attempts an HTTP connection to Meeting Services. In this case, “Enable HTTP Tunneling” must be activated for Meeting Services on the Sametime

server, so that the Meeting Services listen for HTTP connections on the “HTTP Tunneling port” (default port 8081).

If the Web browser’s proxy settings specify an HTTP proxy, the client’s HTTP request is routed through the HTTP proxy; that is, the HTTP proxy server establishes the network connection to the Meeting Services on behalf of the MRC. If the MRC or the HTTP proxy must cross a firewall to access the Meeting Services on the Sametime server, the “HTTP Tunneling port” for Meeting Services (default port 8081) must be open on the firewall.

4.2.4.4 Interactive Audio and Video component connection process

The interactive audio and video components are available in the Sametime Meeting Room client only if the Sametime Multimedia Services add-on is installed. These components connect to Meeting Services and to the Multimedia Multipoint Control Unit (MMCU)/Multimedia Processor (MMP).

To receive and transmit audio and video streams, the MRC and the Sametime server engage in a two-part process. First, the MRC makes a TCP/IP control connection to the Sametime server to exchange call setup and control data. The second part of the process involves the transmission of the audio and video RTP data streams. These streams can be transmitted using either UDP or TCP.

Part 1: Initial call control connection

For the initial call control connection, the audio video components need to talk to Meeting Services. As mentioned before, if another component has already established a connection to Meeting Services, this connection is being reused (see the previous section for details). Otherwise, this connection occurs as follows:

1. The MRC attempts a direct TCP/IP connection to the Sametime server on the “Meeting server port for client connections” (default port 8081) to exchange call setup and control information.
2. If the direct TCP/IP connection fails, the MRC reads the Web browser's proxy settings. If they specify a SOCKS proxy, the TCP/IP connection to the “Meeting server port for client connections” (default TCP port 8081) is routed through the SOCKS proxy. Only connections through SOCKS 4 proxy servers are supported. Connections through SOCKS 5 proxy servers are not supported, since a Web browser’s Java Virtual Machine does not support SOCKS 5. The SOCKS proxy connects to the Meeting Services on the Sametime server on behalf of the MRC. The Meeting Services listen for this connection on the “Meeting server port for client connections” (default port 8081). If the SOCKS proxy needs to cross a firewall to access the Sametime server, this port must be open.

Note

If the Meeting Room client connects to the Sametime server through any type of proxy other than a SOCKS 4 proxy, the transmission of the audio and video streams described in Part 2 below will fail. Audio/video is not supported for clients that connect to the Sametime server through an HTTP, HTTPS, or SOCKS 5 proxy server.

Part 2: Transmitting audio and video streams

The transmission method for the audio and video streams depends on how the initial call control connection was established. The scenarios are described below:

- If the Meeting Room client could successfully establish a direct TCP/IP connection (described in Step 1 above), the Audio/Video Services dynamically select the UDP ports on which to receive audio and video streams from the clients. These dynamic UDP ports are selected from a range of ports specified by the administrator.
- If any firewall or router between the client and the server blocks UDP traffic, the audio and video streams can be tunneled over a single TCP/IP port. This port is called the “TCP tunneling port” (default port 8084). It must be open through all firewalls between the client and the server.
- If the initial call control connection occurs through a SOCKS 4 proxy, the client and server will transmit the audio and video streams through the SOCKS proxy using TCP over the “TCP tunneling port” (default port 8084) as described above.

Note

If the client transmits and receives audio and video streams through the “TCP tunneling port”, up to two separate TCP sockets can be created to accommodate the audio and video streams (two sockets are created for the RTP audio and video streams). These sockets use the same TCP port number. Transmitting the streams over UDP results in better meeting performance than the TCP tunneling method.

4.2.5 Sametime Broadcast client

The Sametime Broadcast client is a signed Java applet that runs in the Java Virtual Machine of the user’s Web browser. Just like the Meeting Room client, it automatically downloads and installs to the local browser environment the

first time a user enters a meeting. The Sametime Broadcast client is also updated automatically on the client whenever there's a new version available on the Sametime server. As a receive-only client, it receives Real Time Protocol (RTP) audio, video and data streams from Broadcast Services on the Sametime server, allowing the users to watch and listen to activity occurring in a broadcast meeting without offering interactive capabilities. This architecture allows for very network-efficient, scalable broadcast meetings, that can include a large number of users (all company meetings, for example).

In order to transmit audio and video streams in a broadcast meeting, the Sametime Multimedia Services add-on must be installed on the Sametime server.

4.2.5.1 Connecting to the Sametime server

The Sametime Broadcast client connects to the Broadcast Services on the Sametime server. The client and server use a call control connection to exchange information about the transmission of the broadcast meeting content. The meeting data is sent as separate streams, one for screen sharing and whiteboard, one or two audio streams, and one video stream. If the presenters are using automatic microphone mode and there are two active presenters speaking concurrently, the broadcast gateway transmits both audio streams. The broadcast client receives these streams from the broadcast gateway and performs mixing of the audio signals if necessary. This section describes details about the network connections, including proxy and firewall issues, involved with connecting to the Broadcast Services and receiving the meeting data streams.

Broadcast client connection process

To receive the broadcast meeting streams, the Broadcast client engages in a two-part process with the broadcast gateway on the Sametime server. First, the Broadcast client makes a Real Time Streaming Protocol (RTSP) connection to exchange call control data. This connection is established either through a direct TCP/IP connection, through an HTTP or SOCKS proxy server, or by using the HTTP connection method. The second part involves the transmission of the screen sharing/whiteboard, audio and video streams. The streams are transmitted over UDP or they are tunneled to the Broadcast client over the initial call control connection using either TCP or HTTP. Both parts of this process are described below.

Part 1: RTSP call control connection

The process for the call control connection occurs as follows:

1. Using a Web browser, the user connects to the Sametime HTTP server on the default HTTP server port (usually port 80).
2. When the user attends a broadcast meeting on the Sametime server, the Broadcast client is downloaded to the user's machine and launches within the Web browser's Java Virtual Machine.
3. The ports on which the Broadcast Services are listening for client connections are passed from the server to the client using HTML.
4. The Broadcast client attempts a direct TCP/IP connection to the Broadcast gateway on the "Broadcast gateway port" (default port 554).
5. If the direct TCP/IP connection fails, the Broadcast client reads the Web browser's proxy settings. If they specify a SOCKS proxy, the TCP/IP connection to the "broadcast gateway port" (default 554) is routed through the SOCKS proxy.
6. If the connection attempt through the SOCKS proxy fails, or the Web browser's proxy settings do not specify a SOCKS proxy, the client encases the connection information within an HTTP request and attempts an HTTP connection to the broadcast gateway. In this case, "Enable HTTP Tunneling" must be activated for Broadcast services on the Sametime server, so that the Broadcast services listen for HTTP connections on the "HTTP Tunneling port" (default port 554).

If the Web browser's proxy settings specify an HTTP proxy, the client's HTTP request is routed through the HTTP proxy; that is, the HTTP proxy server connects to the broadcast gateway on behalf of the Broadcast client. If the Broadcast client or the HTTP proxy must cross a firewall to access the Broadcast Services on the Sametime server, the ""HTTP Tunneling port" for Broadcast Services (port 554 by default) must be open on the firewall.

Part 2: Receiving broadcast meeting streams using RTP

If the initial call control connection described in Part 1 is successful, the client and server determine how to transmit and receive the broadcast RTP streams. Using the initial call control connection, the broadcast gateway sends data to the client that describes the available broadcast meeting streams.

Two variables determine how the client receives the broadcast streams:

- The method by which the RTSP call control connection was established
- The availability of the UDP transport between the client and the server

The most efficient transmission of the broadcast meeting streams occurs when both of the following are true:

- The Broadcast client established a direct TCP/IP call control connection with the Sametime server without going through a proxy server.
- The UDP transport is available through all firewalls and routers between the client and the server.

In that case, the Broadcast client can receive the broadcast streams via unicast or multicast, so the manner in which the client eventually subscribes to the streams depends on the availability of multicast on the user's network:

- The Broadcast client can subscribe to unicast UDP streams. In this scenario, the Broadcast client will dynamically select UDP ports on which to receive the streams. All firewalls and routers between the Broadcast client and the broadcast gateway must pass through UDP traffic.
- The Broadcast client can subscribe to multicast UDP streams. In this scenario, the broadcast gateway dynamically selects the UDP ports on which to send the data. These ports are randomly generated. The client subscribes to a multicast address on a multicast-enabled router and receives the meeting streams from the router. This method requires a multicast-enabled network that allows UDP traffic to pass through all firewalls and routers between the Sametime server and the Broadcast client.

Tunneling of broadcast streams

If UDP is not available on any firewall or router between the client and the server, the broadcast meeting streams are sent to a client using a tunneling method. The streams are tunneled over the call control connection port, and can be tunneled over a direct TCP/IP connection, a connection through a SOCKS proxy server, or a connection through an HTTP server. These tunneling methods ensure that any client that can establish a call control connection with the broadcast gateway can also receive the meeting data streams. The possible tunneling scenarios are described as follows:

- The Broadcast client established a direct TCP/IP call control connection on the “Broadcast gateway port” (default port 554), but UDP is not available between the client and server. In this scenario, the RTP streams are tunneled to the client using TCP over the RTSP call control connection between the client and server.
- The Broadcast client established a call control connection through a SOCKS proxy server on the “Broadcast gateway port” (default port 554). In this scenario, the RTP streams are also tunneled using TCP over the RTSP call control connection through the SOCKS proxy server.
- The Broadcast client established a call control connection over HTTP. In this scenario, the broadcast meeting RTP streams are tunneled through

the HTTP connection between the client and the server on the “HTTP Tunneling port” (default port 554). If the client established the call control connection through an HTTP proxy server, the RTP streams are transmitted through the HTTP proxy on the HTTP Tunneling port.

Note

The Broadcast client can subscribe to broadcast meeting streams in three separate ways (unicast UDP, multicast UDP, or tunneled TCP). It automatically selects the most efficient transport method. The process of selecting the most efficient transport method might require the Broadcast client to simultaneously subscribe to multiple transport methods for a brief period.

Transmitting the streams over UDP results in better meeting performance than the TCP or HTTP tunneling methods described previously.

4.2.6 Sametime-enabled applications

Sametime-enabled Discussion and Teamroom databases make use of Community Services by incorporating “Who is online” and inplace chat room capabilities within the application. The connection process for these applications is beyond the scope of this book. In general, since Sametime-enabled applications are making use of Sametime API components, their connection process is similar to the Sametime Meeting Room client.

For more information about these applications, see the Sametime 2.0 API documentation, available on the Lotus website at:

`http://www.lotus.com/sametimedevelopers`

4.2.7 Other H.323 and T.120 Clients

Sametime 2.0 supports other standards-based H.323 and T.120 clients, which can use Sametime's meeting services and interactive audio video capabilities. Microsoft NetMeeting is a popular example of such a client. The following section describes the required settings to use NetMeeting as a client for Sametime Meeting Services. It also covers the general differences when using H.323 and T.120 clients instead of, or together with, Sametime Meeting Room clients.

4.2.7.1 T.120 Clients

In order to use a T.120 client such as Microsoft NetMeeting for the screen sharing and shared whiteboard portion of a Sametime meeting, the administrator must first enable the option to “Allow people to choose NetMeeting (or other T.120 compatible client) for screen sharing and whiteboard instead of Sametime Web-based meeting tools.” To set this option, go to Configuration -> Meeting Services -> General in the Sametime Admin Tool.

Sametime Meeting Services listen on port 1503 for T.120 connections from Microsoft NetMeeting. This port is used to pass screen sharing and whiteboard data between NetMeeting and the Sametime server. NetMeeting uses the T.120 connection process when connecting to a Sametime server to participate in screen sharing and whiteboard meetings. For more information about the T.120 protocol, see the *Real-time Collaboration Standards* Whitepaper available for download from http://www.lotus.com/sametime

Note: NetMeeting’s built-in screen sharing and whiteboard features can only be used in a Sametime meeting if all participants attend using NetMeeting clients. For screen sharing and whiteboard it's not possible to mix NetMeeting and Sametime Meeting Room clients within the same meeting.

4.2.7.2 H.323 clients

If the Sametime Multimedia Services add-on is installed, it is possible to use Netmeeting as an H.323 client in Sametime audio video meetings, even in conjunction with other Sametime Meeting Room Clients (mixed client meeting).

H.323-compliant clients, such as Microsoft NetMeeting, use the H.323 connection process when connecting to the MMCU on the Sametime server to participate in audio video meetings. This connection process uses the Q.931 protocol for call signaling and the H.245 protocol for call control. To use this type of client, the administrator must “Allow H.323 clients (such as NetMeeting) to join a Sametime meeting.” To enable the corresponding setting go to Configuration -> Connectivity -> Interactive Audio/Video Network in the Sametime Admin Tool.

If enabled, a unique H.323 meeting identifier is created and recorded on the meeting details document associated with each meeting in the Sametime Meeting Center (STConf.nsf). H.323 clients can only join meetings that include an H.323 meeting identifier. A unique identifier is generated for all meetings except those for which password protection or data encryption is enabled.

The Sametime Audio/Video Services listen on the “H.323 server communication port” (default port 1720) for Q.931 call signaling connections from H.323 clients. This port is used when a NetMeeting or other H.323 client attends an audio video meeting on the Sametime server. As a result of the Q.931 call signaling connection, the Sametime Audio/Video Services transmit a dynamic TCP port to the H.323/NetMeeting client. The call setup process then continues on this dynamic port as defined by the H.245 protocol.

Finally, the RTP audio and video streams are transmitted over dynamic UDP ports. All firewalls and routers between the client and the server must allow the transmission of UDP data.

Administrators should also be aware of the following issues:

- H.323 clients cannot be authenticated when accessing the Sametime Meeting Center.
- H.323 clients do not support Sametime encryption.
- There is no proxy support for H.323 clients. H.323 clients cannot connect to the MMCU on the Sametime server through any type of proxy server.
- Any H.323 client that connects to the Audio/Video Services must have “silence detection” enabled. Microsoft NetMeeting has silence detection enabled by default. H.323-compliant clients without silence detection enabled can significantly increase CPU usage on the Sametime server and degrade meeting performance.
- In a mixed client Sametime meeting, only the audio/video portion is available to both Sametime Meeting Room clients and H.323-compliant clients.
- If the environment includes an H.323 gatekeeper, H.323 clients can connect to the Sametime Audio/Video Services through the H.323 gatekeeper. For more information, see “Connecting to the Audio/Video Services through an H.323 Gatekeeper” in the Sametime 2.0 Administrator’s Guide.
- If the network includes an H.323 gateway, PSTN users can also call into an audio/video meeting.

In general, other H.323 or T.120 clients such as Microsoft NetMeeting do not support connections to the Sametime server through SOCKS or HTTP proxy servers. When a NetMeeting user connects to the Sametime server through a firewall, all firewalls between the client and the server must allow connections on the ports listed above.

More information about the T.120 and H.323 protocols can be found in the Whitepaper “Real-time Collaboration Standards” which is available on the web at `ftp://ftp.lotus.com/pub/lotusweb/product/sametime/ST_standards.pdf`

4.3 Putting it all together: Sametime 2.0 architecture overview

Finally, Figure 43 gives an overview of the Sametime 2.0 architecture, including the main client and server components.

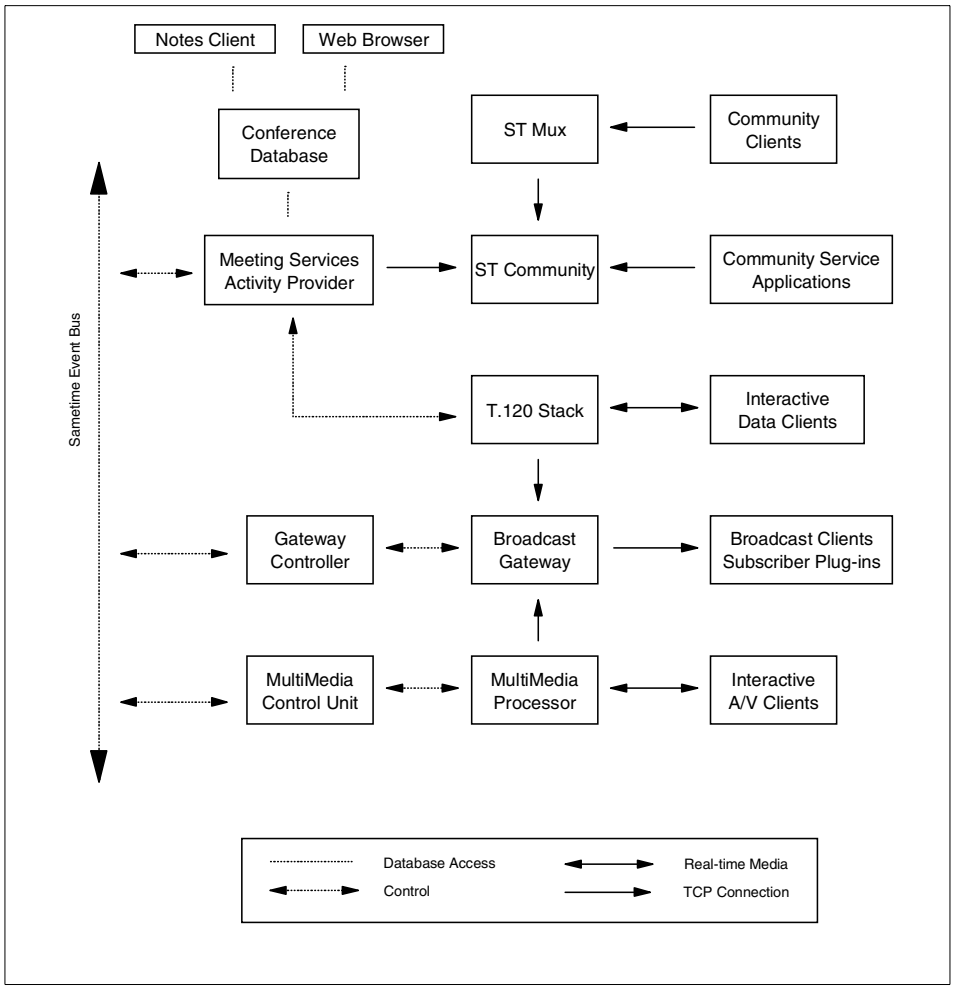


Figure 43. Sametime 2 architecture

For a detailed explanation of each of these components, please refer to the preceding sections.This concludes our exploration of the inner workings of the Sametime architecture.

4.4 Security considerations

Any Sametime administrator should be familiar with the security concepts of Sametime. The Sametime Administrator's Guide covers the security topic in sufficient details, so in general this material will not be repeated here. Instead, we'd like to point out a few things and give some recommendations regarding Sametime security.

4.4.1 Secrets and Tokens authentication

In order to avoid multiple prompts for username and password, many Sametime applications, including the Sametime Meeting Room and Broadcast clients, use the Secrets and Tokens authentication system.

We strongly recommend to enhance the security of any Sametime installation by running the SametimeSecretsGenerator agent in the Secrets database on the Sametime server at least once, even if you don't plan on running the agent periodically. In a multi-server environment, this agent should be run on the first Sametime server prior to the rollout of the secrets database (STAuthS.nsf).

More information about running the SametimeSecretsGenerator agent can be found in the "Enhancing security" in the Sametime Administrator's Guide.

4.4.2 Single login solutions

If you have multiple access-controlled Sametime-enabled Web applications running side by side with non-Sametime Web applications on a Domino server, you may want to provide a single login solution for your browser users in order to prevent multiple prompts for username and password.

For browser-based access, Sametime uses a two-level authentication system, where the authentication of the Sametime-specific client components via the Secrets and Tokens mechanism basically sits on top of the underlying http authentication. So, in order to provide single login for the Sametime applications, the key is to provide single login for the http authentication.

The core http stack in Sametime is provided by a Domino server, so all Domino-specific techniques apply here as well. Among them are:

- Using Domino Web realms

- Writing a DSAPI filter
- Using session authentication

4.4.2.1 Domino Web realms

Using a Domino Web realm, you can specify a text string that is displayed when users try to access a certain drive, directory, or file on a Domino server. When the browser prompts the user for a name and password, the browser's authentication dialog displays the realm text string. The browser uses the realm to determine which credentials (user name and password) to send with the URL for subsequent requests.

The Domino Web server caches credentials for different realms to avoid prompting the user again for the same credentials. The realm string also applies to requests mapped to paths that have the specified path as their root, provided that the child paths of the root do not already have a specified realm.

For example, the realm string specified for d:\domino\data also applies to a request mapped to d:\domino\data\userapps, if the latter does not have a specific realm specification.

Example:

A Domino server (domino.fishnet.com) holds several access-controlled web applications in separate data subdirectories. Anonymous access is disabled, so in order to access the data, a browser user must first authenticate.

The structure of the data subdirectories is as follows:

```
d:\domino\data\apps\nonstapps\app1.nsf  <-- web application 1
d:\domino\data\apps\stapps\app2.nsf     <-- web application 2
d:\domino\data\apps\morestapps\app3.nsf <-- web application 3
```

Because the Web applications are placed in different subdirectories, normally the browser would prompt the user for username and password for each of the applications. By creating a Domino Web Realm document for the d:\domino\data\apps\ directory, all applications within and below that directory will be treated under the same Realm. So, once a user authenticated with any of the applications (for example app2.nsf), he or she will not be prompted again to authenticate with any other application living in or below d:\domino\data\apps\ (for example app3.nsf).

Figure 44 on page 116 shows the corresponding Web Realm document in the Domino directory.

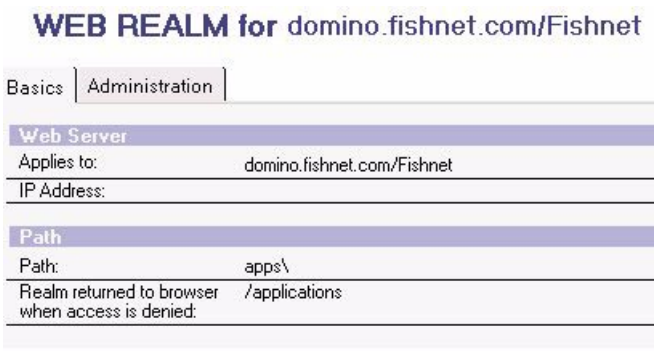


Figure 44. Web Realm document

For more information about Domino Web Realms see the Domino Administrator's Guide.

4.4.2.2 DSAPI filter

The Domino Web Server Application Programming Interface (DSAPI) is a C API for writing extensions to the Domino Web Server. A DSAPI extension (or filter) is a custom written program routine that is notified when certain events occur on the Web server, such as when a URL request is received or when a user is about to be authenticated.

Intercepting the http authentication process is especially interesting if you want to complement or replace the Domino internal http authentication mechanism, for example by checking the user-provided credentials against a legacy mainframe system. The DSAPI program could then parse the user name, check the user name and password against the legacy mainframe system, and, if successful, notify the Domino Web server that it has handled the authentication event, and pass Domino the distinguished name of the user.

For more information about DSAPI filters, see the redbook *Lotus Notes and Domino R5.0 Security Infrastructure Revealed,* SG24-5341.

4.4.2.3 Session authentication

A session is the time during which a Web client is actively logged on to a server. Session-based name-and-password security includes additional functionality that is not available with basic name-and-password security:

- A **customized HTML log-in form** allows a user to enter a name and password and then use that name and password for the entire user session. The browser sends the name and password to the server using

the server's character set; therefore, a user can enter a name and password in a character set other than ASCII or Latin-1. Domino provides a default HTML form, which is created and configured in the Domino Configuration database (DOMCFG.NSF). You can customize the form to contain additional information.

- Specify a **default log-out time period** to log the Web client off the server after a specified period of inactivity. Automatically logging a user off the server prevents others from using the Web client to impersonate a user if a Web client leaves the workstation before logging off. Users can also append ?Logout at the end of a URL to log off a session (for example http://domino.fishnet.com/apps/stapps/app2.nsf?Logout).
- Control server performance by specifying the **maximum number of user sessions** that are allowed on the server at the same time. If the server performance is slow, you can reduce the number of active user sessions that can occur on the server concurrently.

Setting up session authentication is simply a matter of adjusting the server document in the Domino directory. As of Domino 5.0.5, Domino also provides multi-server session authentication, which allows for cross-server single login solutions.

To use multi-server session authentication, you have to create a Web single sign-on configuration document and adjust the Domino server settings. So, the easiest way to achieve a cross-server single login solution for Web applications running on both Sametime servers and Domino servers is to run Domino 5.0.5 on all of your servers and install Sametime on top of Domino for your Sametime servers.

Note

To use session-based authentication, Web clients must use a browser that supports cookies because Domino uses cookies to track user sessions.

If your servers are set up for round-robin DNS, do not use session-based name-and-password authentication. The servers cannot store the session information in memory when using round-robin DNS. In addition, if a server is restarted or crashes, session information is lost. Then the user must re-enter the name and password.

For details about how to set up session authentication, refer to the Domino Administrator's Guide.

Figure 45 and Figure 46 show the corresponding Web single sign-on configuration document and the settings in the Domino server document necessary to support multi-session authentication.

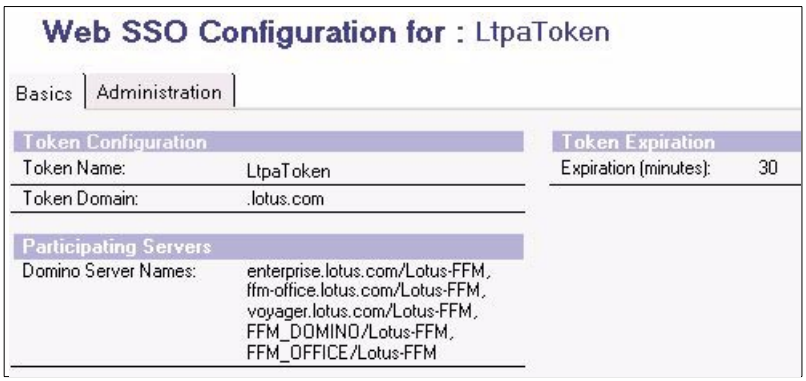


Figure 45. Web single sign-on configuration document settings to support multi server session authentication

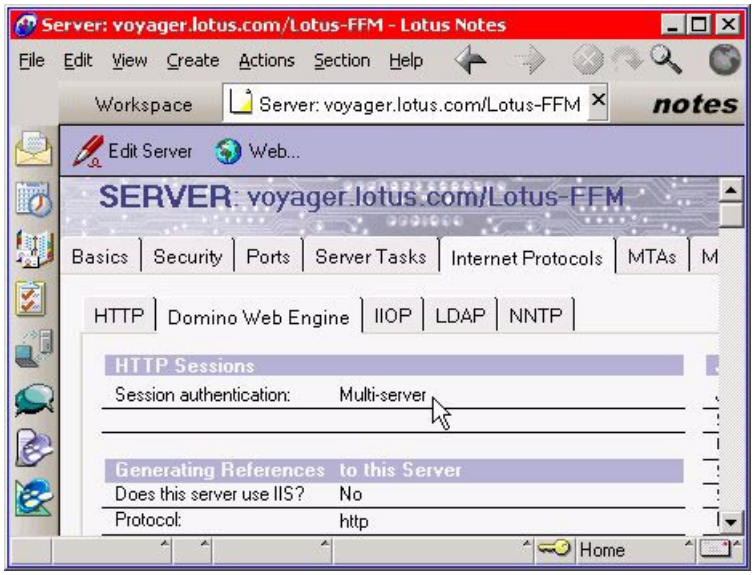


Figure 46. Domino server document settings to support multi server session authentication

4.4.3 Encryption

At the time this redbook was written, the Domino DNA kernel in Sametime 2 was based on Domino 5.0.3. Beginning in Release 5.0.4, the Domino server is available as a single “Global” release, which provides for stronger

encryption. This is especially interesting for international customers, as previous international versions of Domino did not offer 128 bit SSL encryption without using an externally provided Global server ID, which customers had to order from Verisign.

For more information about Global server IDs, see:

`http://www.verisign.com/cus/srv/faq/g/other.html`

For SSL, Domino 5.0.4 and higher offer the following encryption strength without the need for a Global server ID:

- 1024 bit RSA key in the web protocols (SSL and S/MIME)
- 128 bit encryption (SSL and S/MIME)

If you use SSL on your Sametime server and want to use these stronger encryption capabilities, you should consider running Sametime on top of a Domino 5.0.4 (or higher) server, because in this configuration, Sametime uses the existing Domino kernel and doesn't install its own Domino 5.0.3 DNA kernel.

4.5 Extending a Sametime Infrastructure

This section describes useful real-world examples of how you can enhance an existing Sametime 2.0 infrastructure with new services.

We describe the Lotus Translation Services for Sametime, which introduce on-the-fly, multi-language translation capabilities for users in a Sametime community. Then we describe how Sametimes awareness and instant messaging capabilities can be extended to mobile phones using WAP technology.

4.5.1 Lotus Translation Services for Sametime

An add-on product to Lotus Sametime, the Lotus Translation Services for Sametime (LTSS) lets users collaborating within a Sametime community conduct multilingual chat sessions. Using the Lotus Translation Components as the underlying back-end architecture, the LTSS connects to Translation Servers via supported Translation Connectors developed by IBM or third party vendors.

4.5.1.1 Overview

The Lotus Translation Services for Sametime is a Client/Server Java application that runs within the Sametime community.

It consists of 3 main components:

- Server application
- Translation Console
- Configuration and Administration database

4.5.1.2 The server application

Implemented as a Java-based standalone component, the LTSS server application runs within a Java Runtime Environment (JRE). It launches as a console application and presents a command line interface, accepting administration commands from the console input.

The server displays significant events and the output from commands entered on the command line console. Using the Sametime client API, the server application logs into the Sametime community using any predefined alias (by default the alias is “Translation Services”). Once running, it appears as that user in the Sametime Connect buddy list and can be invited into single or multi-user chats.

4.5.1.3 The Translation Console

Sametime users can get translation services by inviting the aforementioned user (Translation Services) into a chat. This returns an instant message with a URL link to the Translation Console. The Translation Console is actually a Java applet launching in the default browser. It provides for the translation of chat sessions and offers dictionary look-up capabilities.

The user can specify languages for reading and writing. Depending on the user’s preferences and the available translation services in the background, it is also possible to choose from different subject dictionaries. The original message as well as translated chat messages appear in the translation console, so the translation process doesn't interfere with the original chat session.

Figure 47 on page 121 shows the Translation Console with a sample chat, including translations from English to German using a general style subject dictionary.

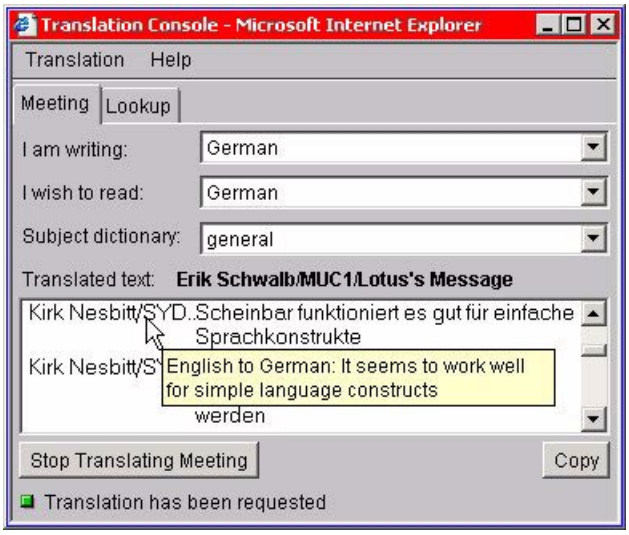


Figure 47. Lotus Translation Services for Sametime: Translation Console

The LTSS lets initiators and invitees of chat sessions translate any chat sessions they participate in. It works in both one-to-one and multi-party chat sessions.

4.5.1.4 Configuration and Administration database

The Configuration and Administration database is used to:

- Launch the LTSS Translation Console
- Access the LTSS User Guide
- Remotely administer the LTSS Server using the Remote Administration Console

The *Remote Administration Console* is modelled on the Domino R5 remote console. From the console the administrator can type commands and send them to the server. It supports both Sametime 1.5 and Sametime 2.0 servers.

The Translation Console and the Lotus Translation Services for Sametime Configuration and Administration Web page are available in French, German, Italian, Spanish, Dutch, Finnish, Norwegian, Danish, Portuguese, Simplified Chinese, Traditional Chinese and Japanese.

The LTSS connects to any translation server supported by the *Lotus Translation Components* via Translation Connectors. Supported vendors are

IBM, Transparent Language, Systran and Lernout & Hauspie. This allows customers to choose a vendor according to their individual translation needs.

Fore more information about the Lotus Translation Components go to:

`http://www.lotus.com/international`

4.5.2 Sametime for WAP

By extending Sametime to mobile devices such as PDAs and mobile phones, business people can stay in touch no matter where they are. The Sametime for WAP application has been developed by Lotus EMEA specifically for the European market, where digital mobile phones based on the GSM standard prevail, and where all mobile phone service providers are interconnected, offering transparent roaming services.

Sametime for WAP offers Sametime Connect functionality for a WAP-enabled mobile phone or any device that supports the Wireless Application Protocol 1.1 (WAP 1.1). Mobile users can search for people in the Lotus Sametime directory, create and manage buddy lists, see who is online (awareness), and send and receive instant messages via live chat functionality.

The overall architecture consists of these main components:

- Sametime server
- Domino server running the Sametime WAP engine
- WAP Gateway
- Dial-up network service (either company internal or provided by an ISP)
- WAP 1.1 compliant mobile device

Figure 48 on page 123 shows an overview of the infrastructure components necessary to implement a Sametime for WAP solution.

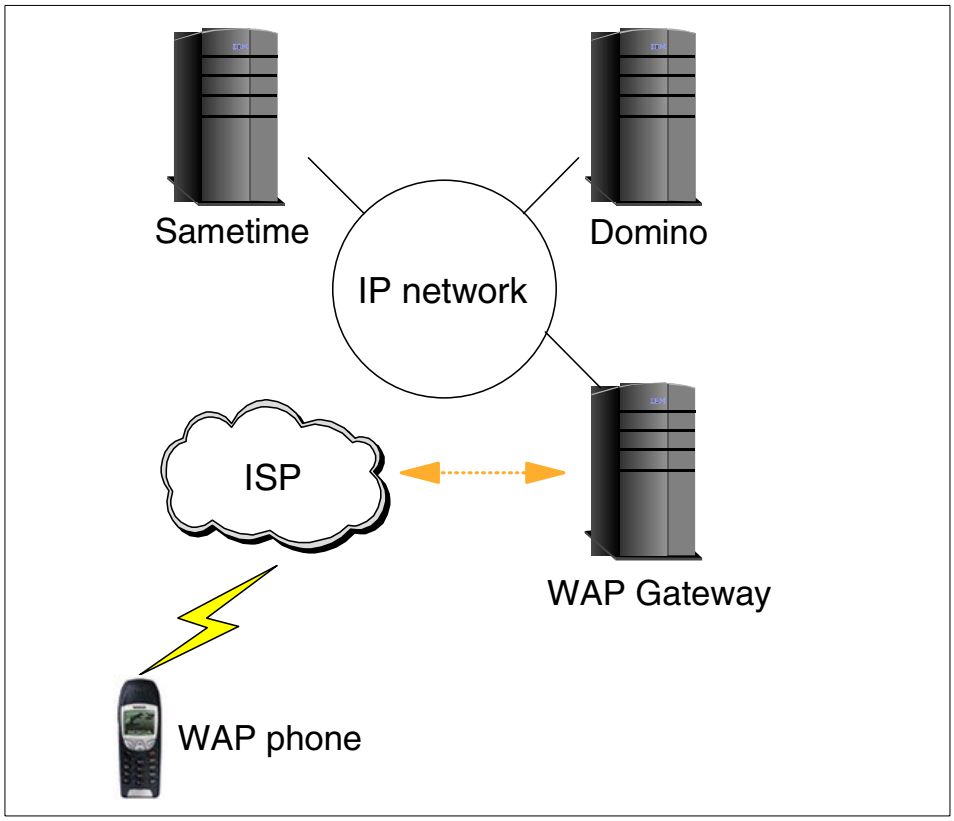


Figure 48. Sametime extended to WAP phones

Running on a Domino server, the Sametime WAP engine acts as a proxy for the Sametime users who connect via the WAP Gateway. It's a multithreaded servlet-based engine, which can handle multiple concurrent connections. Also on the Domino server is a configuration database, which stores global settings, user buddylists, and profile information.

The following figures show a typical session for a Sametime for WAP user on a mobile phone. The figures have been created using a mobile phone emulator which behaves just like “the real thing.”

Like any other browser-based Sametime client, the Sametime for WAP service can be reached via a URL. So, after dialup to the network, the mobile phone user has to provide their username and password. These are the same values used for Sametime Connect, and as such, they are checked against the username and internet password fields of the person record in the Sametime directory.

The login dialog looks like Figure 49.

Figure 49. Sametime Login on WAP phone

On a PC, a Sametime for WAP user appears in Sametime Connect's buddy list just like any other Sametime user, as shown in Figure 50.

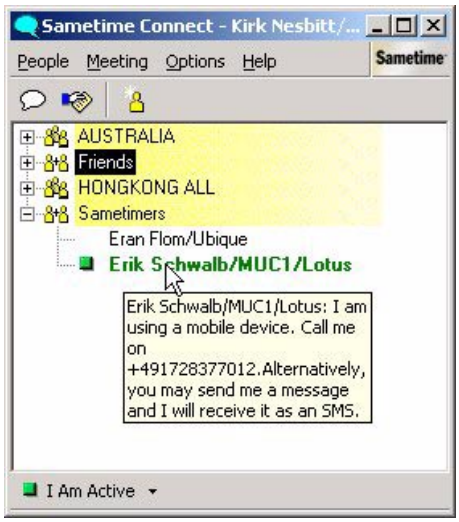


Figure 50. A Sametime for WAP user listed in the Sametime Connect buddy list

The extended Online Status Message ("I am using a mobile device. Call me on...") shown in Figure 50 is composed automatically after the Sametime for WAP user has filled out a profile containing their mobile phone number and SMS e-mail address. By using typical Domino application development tools, the phone number in this profile could also be derived from the person record in the Sametime directory.

As WAP 1.1 currently doesn't allow you to trigger a connection from a server to a mobile device, it's not possible to initiate a chat from a PC based

Sametime client or any other mobile Sametime user to a Sametime for WAP user.

However, by adding the messaging capabilities from Lotus Mobile Services for Domino (MSD), Sametime Connect users on a PC can send SMS messages to Sametime for WAP users.

Trying to initiate a chat with a mobile user from a Sametime Connect client results in the system-generated message shown in Figure 51.

Figure 51. Auto generated message

After login, the mobile user is presented with their buddylist, which is kept on the server. Just like the PC-based Sametime Connect client, the buddylist on the WAP device shows selected people and their online status, as shown in Figure 52.

Figure 52. Sametime buddylist on WAP phone

The meaning of the status symbols is as follows:

```
o = online
x = offline
AW = away
```

In contrast to PC-based Sametime clients like Sametime Connect, the online status of a mobile user persists—even if the mobile phone is switched off—as long as the user doesn't explicitly log off from Sametime via the mobile phone or log into Sametime from any other PC-based client.

After selecting a specific user from the buddylist, a Sametime for WAP user can "Request a phone call," as illustrated in Figure 53.

Figure 53. Options for selected user

Figure 54 shows the confirmation message on the mobile phone.

Figure 54. Phone call request send

This action results in a pre-defined message being sent to the selected user, asking them to place a phone call to the mobile phone number, as shown in Figure 55.

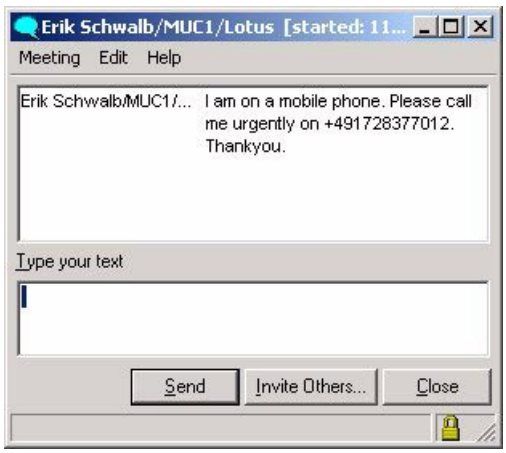


Figure 55. Incoming phone request

It's also possible to initiate a regular chat by sending an instant message, as illustrated in Figure 56.

Figure 56. Sending an instant message

To get the answers from the instant messaging partner, the WAP device refreshes the display at a user-definable interval. Figure 57 on page 128 shows what a regular chat looks like.

Figure 57. Sametime chat on a WAP phone

Sametime for WAP is available from Lotus Professional Services (currently in Europe, Middle East, Africa, Australia and South America) as part of a service offering called Sametime Everyplace Quickstart. For more information about the Wireless Solutions Portfolio contact your local Lotus representative.

In this section, we introduced the Lotus Translation Services for Sametime, which provide on-the-fly, multi-language translation capabilities for users in a Sametime community. We also described how an existing Sametime infrastructure can be extended to provide awareness and instant messaging capabilities for mobile users on WAP devices.

Chapter 5. Sametime clients

This chapter describes the three types of Sametime client programs and some of their functions. It covers some of the more interesting features of each program, as well as some general issues related to the use of Sametime.

For more details, consult the *Sametime Installation Guide* or the online help files contained within the Sametime clients.

There are three types of clients: Sametime 2.0 Connect client (Connect), a Java based JNI application called the Meeting Room Client (MRC), and a lighter “Broadcast” Client (BC) that is also a Java applet.

5.1 Connect client (Connect)

The full Sametime Connect 2.0 client is a C++ Win32 program that resides on each user’s PC. When active, Connect keeps the connection to the Sametime servers for instant messaging and online awareness updated on your current status. This is known as “community” or awareness.

The client also determines (through prompts) what services and functions are available on your PC (camera, microphone, speakers) and if they are supported on the Sametime server, and adjusts local menu options accordingly.

It is installed in C:\Program Files\Lotus\Sametime Client by default.

Note

There is work under way to create a complete Java-based 2.0 Connect client, but as of the writing of this book, it does not exist in any published form. However, you can obtain a working 1.5 Java version for community awareness and text messaging from `http://www.lotus.com/sametime`

5.2 Meeting Room Client (MRC)

The MRC is a Java-based application that is downloaded and executed locally. The application is cached to speed future startups, and is also self-updating when updates are loaded on the server. The MRC has all the functions required for any meeting service requested, but does not maintain community awareness beyond the meeting it is attending.

Note

MRC uses 2 native Windows application calls (via JNI) for video and keyboard functions, so its is not a cross-platform Java application.

5.3 Broadcast Client (BC)

The BC is a thinned-down version of the MRC that allows only viewing and listening to a broadcast meeting, and does not have any interactive functions such as chat or text messaging. It is a much smaller download for clients attending a meeting using this applet.

This client is downloaded at the time you attend the meeting, and is cached for re-use at a later meeting. Updates (if any) are automatically obtained from the Sametime server.

5.4 Client use notes

Following are some issues to be aware of when you use the Sametime clients:

- You can use H.323 standard programs such as Microsoft Net Meeting for online meeting functions. However, you cannot use them for community awareness, instant messaging, or instant meetings.
- There are no options for controlling the colors and fonts in the Sametime Connect, MRC or BC. All defaults come via the Windows Control Panel options for colors and font sizes.
- It is important to set your microphone to a proper sensitivity level when using Automatic microphone mode. If it is too sensitive, the microphone will pick up background noise and breath sounds, which can result in the audio and video controls switching indiscriminately during a meeting. Use of the Mute switch on screen or on your microphone is a good idea whenever you are not speaking.

Complete instructions can be found in the online help files included with the clients.

5.5 Browser requirements for Sametime

When you use Sametime to access an on-line meeting (text IMs are the only exception), you are actually using your Web browser and the Java functions for all Meeting Room Client or Broadcast Client services.

Except as noted, it is not required to have the Connect client running—or even installed—to start or attend a online meeting. (For a Netscape user to be able to share their own PC with others in the meeting, a Netscape plug-in is required before starting.) The Connect client is used for community awareness and instant messaging services throughout the day. It also provides a alternative launch point to start application and AV meeting.

You can launch all meeting services through the browser. This means that anyone with access to the Sametime server website can start using Sametime without doing any installations.

Netscape 4.5 or IE 4.01 (SP2 or higher) are required. No other browsers (including the Notes Browser) are supported at this time. We tested Notes and Opera 4.02 and were greeted with “Browser Not Supported” when attempting to book a meeting.

5.5.1 Netscape plug-ins for Connect

In order for a Netscape 4.5 (or higher) user to be a full participant in a collaborative meeting, a Netscape plug-in (NPDBAS.DLL) is required to enable that user to share his desktop display with others. This plug-in allows the local PC screen to be displayed to and remotely controlled. It is not required for any other Sametime function, and without it, a Netscape user still can attend, see A/V, use the whiteboard, chat, and view other’s shared sessions.

The Connect 2.0 client install process will add this plug-in to the default Netscape directory, if the directory is found during the installation.

By default, Netscape plug-ins are placed in:

C:\Program Files\Netscape\Communicator\Program\Plug-ins

You can confirm the presence of the plug-in by looking in Netscape under Help -> About Plug-ins, and looking for an entry that looks like Figure 58.

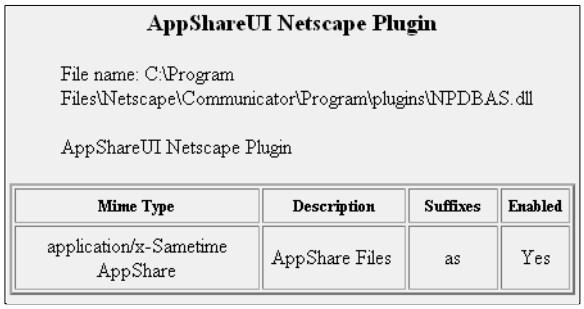


Figure 58. Netscape "About Plug-ins" panel

Net Meeting plug-in

If you plan to use Net Meeting to receive audio/video broadcasts instead of downloading the Broadcast Client, this plug-in allows Net Meeting to be directed by the Sametime meeting server.

You can install this as a download executable file from the Sametime server. It can also be included in the customized Sametime Client packaging process, as described in 1.4, "Sametime client packager" on page 19.

Sametime Print Capture

This utility allows you to "print to file" from any application you wish to share output from at a later meeting. Use it to print from any application. It appears as another printer in the Windows Printer folder, as shown in Figure 59.

Figure 59. Sametime Print Capture in Control Panel - Printers listing

It creates a file output for Sametime meetings to load into the whiteboard. You must use it before booking your online meeting. Then load those created files (FST is the extension they are created with) into the meeting when booked.

This Print Capture utility is useful if you have files that cannot be natively understood by the Sametime meeting manager when you book it.

5.5.2 Internet Explorer plug-ins for Connect

When you use Microsoft's Internet Explorer (4.01 SP2 or higher), there is no need to pre-install a plug in. All plug-in services are done automatically on demand (unless you have this turned off for security reasons; then you must grant permission first).

Because of the automated nature of the plug-ins, Internet Explorer 5.0 seems to function slightly smoother with Sametime's MRC than Netscape 4.75 at set-up, though both function equally well once set-up is complete and the meeting is started.

5.6 Sametime Connect client services

Sametime Connect client has two basic services contained within it: community services and meeting services. Each service has several functions that operate within it.

5.6.1 Community

There are three functions provided by the Sametime Connect client to the community service servers. They are:

- Community awareness

  This is a constant update to the server and other users concerning your status: on/offline, Available, Away, or in Do Not Disturb (DND) status. It is the key for database awareness applications. It also provides the basis for text-based Instant Messaging (IM).

- Instant messaging

  By default, all IMs are text-based messages. These can be sent to any person who is online and who you are allowed to see. An exception to this is when you use DND. In this case users will see you, but will be unable to send IMs to you. You will not know that an attempt was made.

  Audio and video IM requests can be sent the same way, except that instead of the initial message appearing, you are sent an invitation to join an instant meeting when audio and video services are then set up.

- Instant meetings

  These are hosted on the Sametime community servers, just as a scheduled meeting is, but without requiring that you go to the "reserve a meeting" Web process. Once started from the Connect client, you are connected to the meeting services section of Sametime. You can start an

instant meeting either as an invitation sent to people in your buddy list, or as a continuation of a IM session started earlier.

5.6.2 Meeting services

Four functions are provided in the Meeting Room Client. They are:

- Whiteboard

  This feature allows you and others in the meeting (with permission granted by the moderator) to see panels, such as Freelance or Powerpoint slides, that were pre-loaded for the meeting. It also lets all users annotate in freehand on top of the panels, or work on a blank whiteboard. Note that annotations and drawings cannot be saved natively. A screen capture utility or Print Screen function would be needed to save any items you may want to keep.

- Meeting Room IM

  This feature is restricted to meeting attendees and appears in a chat room format. Text transcripts are not saved, nor are they viewable by others outside the meeting session. You can also launch private chat windows with other participants within the same meeting, but not with anyone outside (unless you use your Connect client program to do so).

Note

When using the MRC to attend a meeting, your online status will be visible to all users in the Sametime community. The MRC does not allow you to change your online status. However, the MRC will display the status set in your Connect client, if active.

We recommend running the Connect client at all times to control your status message. Outsiders cannot see who or what is going on in the meeting when they message you.

- Screen sharing (application sharing)

  This allows you to see other user's PC desktop, a specific window, or a selected area of their screen. You can also share your desktop with others and let them remotely control your desktop applications. The sharing user can stop this at any time.

- Audio/Video services (if Multimedia services are installed)

  This is the advanced voice and video interaction function of Sametime. To keep the meeting orderly, you can have either an "Automatic microphone,"

which senses and switches among the speakers; or a “Moderated microphone,” which either automatically queues users in the order in which they requested to speak, or queues users at the moderator’s command. The video display follows the active speaker. If there is no video available, the Sametime logo panel will be displayed.

The Broadcast Client (BC) also provides these five functions, but in a “watch only” mode that cannot be changed.

The meetings types that make use of these functions are described in the next section.

5.7 Sametime meeting types

There are 3 types of meetings that can be conducted in Sametime. They are all set via the Sametime Web interface.

5.7.1 Full collaboration

A full collaborative meeting is likely the most common type you will encounter. All participants have 2-way interaction with all presentation, talk, and discussion. It is best suited to small groups, and is also the definition for one-on-one instant meetings.

A full meeting defaults to allow all users access to whiteboard, screensharing, audio, and video functions (if available). The microphone is in “automatic” mode by default. The meeting manager still can control the meeting, if needed, by granting and revoking specific function rights.

This type of meeting is not recommended for groups larger than 10 or so, as it places the heaviest demand on the network and servers. And any meeting with more than a few people trying to talk at once can be very confusing.

5.7.2 Moderated meeting

A moderated meeting is one where the meeting manager (usually the meeting creator, or it can be designated at booking) has full control of meeting functions. All others gain control of the functions at the moderator’s discretion, or if pre-set when the meeting is booked. A product demonstration is a good example of this type of meeting.

Moderated meetings allow specified participants (those with the rights granted by the moderator) to use the whiteboard, audio/video, and screen sharing.

All other audience members do not have those functions presented to them unless granted by the moderator from the meeting menu control panel. When granted access to a specific function, that function will appear on the speaker's screen automatically.

5.7.3 Broadcast meeting

A broadcast meeting (such as a CEO address to all employees) is the largest type of meeting Sametime can hold. It is controlled by one presenter and is transmitted via a one-way client interface (the BC) that does not allow the general audience any interaction (much like a TV broadcast). You cannot grant interactive functions to users via the BC.

This type of meeting would most often consist of an audio and video broadcast, along with a screen presentation. It makes full use of IP multicasting (if enabled) and the broadcast gateway services.

5.8 Sametime Connect client features

The Sametime Connect client has a simple interface, with all available options displayed as icons on the top bar, along with pop-up prompts. If a functions (such as video) is not available, the icon and associated menu items do not appear at all.

All functions are documented in the Sametime Users Guide. Access this information by selecting Help -> Help Topics on the Sametime Connect client menu. Some of the functions are described here.

Figure 60 shows the Connect client main interface.

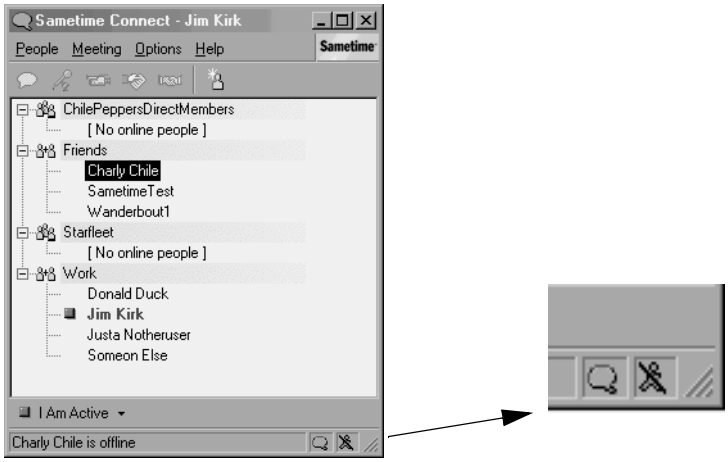


Figure 60. Sametime Connect client - main panel, with on/off line indicator highlight

AOL and Sametime names can now be kept in the same group. They still can't interact in the same conversations.

Online/Offline indicators - Status is indicated by a slash to show no connection. You can no longer click on the icon to begin a login. You must use the menu items.

Status messages - Right-click in the Sametime icon in the system tray to access the status settings of Sametime, as shown Figure 61.

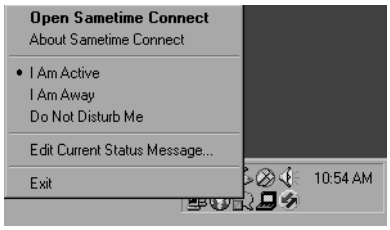


Figure 61. Sametime Connect client: right-click menu from system tray icon

The status is now reflected in the System Tray icon with a matching, colored icon to reflect whether you are Active, Away, Do Not Disturb, Connecting, or Disconnected. A pop-up menu shows your current status message.

Note

When you chose the “Edit Current Status message” check box option in Sametime 1.5 your status message did not change until you clicked OK or canceled the edit. In 2.0, the status changes immediately and the edit box can remain open.

Directory services, under the Add Person option, is displayed in Figure 62. You must be logged in to Sametime to add or look up users since all directory queries are passed through the Sametime servers first. For AOL names, you must be logged in, though AOL will not attempt to validate the names you enter.

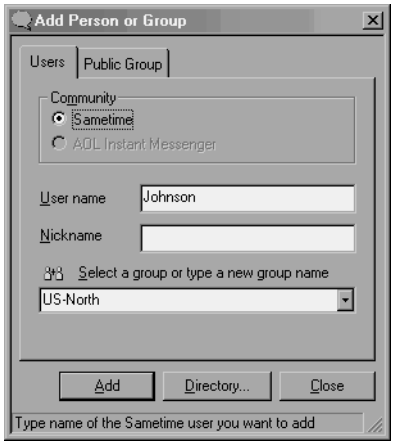


Figure 62. Sametime Connect client AddPerson or Group panel

You can also use the extra menu items under People -> AOL Instant Messenger Services to register, reset, or look users up by e-mail address. If you are not connected to AIM, the selection item will be shaded out.

The Sametime icon’s appearance in your Windows system tray now reflects your online status, with changing icons, pop-up status, and the ability to edit the status message via a right-click menu.

Note

When the Sametime Client is minimized, it will no longer appear on your Windows task bar, nor will be be in your ALT-TAB listing. You can recall it by double clicking on the Sametime icon appearing in your system tray. If you use an icon to launch the session, the first session will be restored as the active window again.

5.8.1 Connect client security

By default, IM text messages in Sametime Connect are encrypted by the client using an RC2 40 bit International key. Meetings and audio/video data streams can also be encrypted if the option is selected when booking the meeting (under the Security tab when booking a meeting).

It is recommended that you generate a new security key when installing ST servers. A default security key is provided during the install.

The ID and passwords exchanged between Sametime servers and the Domino or LDAP directory services are capable of 128 bit encryption if you set them up to use SSL at installation.

Users can save any chat transcript to a text file. This must be done manually by selecting the active chat window, then choosing Meeting -> Save As. This will store the current chat transcript to a plain text file in the default folder shown. The default name is your user ID and the date/time the message started.

There is no method of logging or tracking messages as they pass through the Sametime servers.

5.9 Connect client privacy settings

Sametime Connect allows you to exclude other Sametime users from seeing you as “online” and thus lets you prevent them from contacting you. You select this setting from Options -> Who Can See If I Am Online. The interface looks like the one shown in Figure 63 on page 140.

Figure 63. Sametime Connect client - Who Can See If I Am Online settings panel

From here you can add or remove names, and set whether each is to be included or excluded from seeing you online.

Sametime privacy lists are stored on the Sametime server (in VPUSERINFO.NSF under several “privacy views”). Using this option allows you to control who can and cannot see you online. Blocked users will display as “off-line” and you will appear as “off-line” to anyone you block, too.

We recommend that you use privacy settings only for short, deliberate periods of time and otherwise default to “Everybody can see me online” for normal use.

Do not attempt to edit the privacy settings from within VPUSERINFO.NSF on the server. Use the Connect client for all updates and changes.

Note

Take note that when you exclude a user from seeing you online, it also prevents you from seeing them online. Privacy is a two-way street in Sametime.

5.10 Sametime chat rooms

Sametime does not natively support persistent chat rooms. You can conduct a temporary chat session by inviting all parties into a IM text conference chat.

If a person leaves the meeting, they must be invited back in by one of the remaining attendees.

However, you can work around this issue by booking regular open meetings.

Set up a scheduled meeting in Sametime that is repeated daily (use the Repeat button on the Essentials tab when booking a meeting).You can even password protect meetings to keep unwanted users out. The meeting specifications can be modified and moderated at any time by the meeting owner/moderator to allow whiteboard, application sharing, and A/V functions.

In any meeting, it is not possible to review any text conversations that may have taken place before you entered. However, transcripts can be saved by any attendee, and forwarded to you as an e-mail attachment later.

For other “open chat” styles of meeting, we suggest you look to products such as Lotus Quick Place or TeamRoom databases for this service.

There are API interfaces that can allow you to set up customized open chat services as a separate application. You can obtain the sample code and toolkit that lets you see how Sametime can be extended. Find the code and further details in the Developers section of the Lotus Sametime website at:

`http://www.lotus.com/sametime`

5.11 Domino/Notes applications

Sametime can interface with other Web applications and Domino databases to give you a view of other users who are accessing the same files as you. This means that you can have a team database where you and others might be in the same sections. Sametime lets you “see” each other as on-line there, and you can send them an instant message right from that indicator to discuss the file in question further, and from there, you can also start a meeting session if desired.

Sametime-enabled teamroom and discussion database templates (STTEAM.NTF, STDISCUSS.NTF) are included in the standard installation for you to try. If you plan on utilizing these templates, we recommend installing them to a Domino database server. Placing them on the Sametime server will reduce resources if they are used regularly.

The Sametime 2.0 Toolkit for developing Web and Domino applications using Sametime functions is available from Lotus.

Also, see the redbook *Lotus Sametime Application Development Guide for Sametime 1.5,* SG24-5651 for more details.

5.12 Sametime 1.5 to 2.0 client upgrade issues

There are a few items of note if you will be upgrading Sametime clients to 2.0 from 1.5.

A full list of what's new in Sametime 2.0 can be found in the Sametime Administrators Guide included with the Sametime package.

- At this time, we recommend uninstalling any old versions of Sametime Connect client before installing 2.0. Local settings in the connect.ini and userid.dat will not be removed.
- A Sametime 1.5 client will work on 2.0 servers. However, they will not be able to start audio/video instant meetings.
- The settings and buddy lists will migrate to Sametime 2.0 with no problems. Buddy lists will not migrate backward to 1.5 though, as the file format has changed slightly.
- Sametime 1.5 applications and functions are forward compatible with 2.0.
- Any application written to 1.5 will work with 2.0. However, any applications written in 2.0 format may not work with 1.5 clients.

5.13 Sametime buddy lists

Sametime uses a list to keep your personal contact names or "buddies" for the Connect client to display status on after you log in. In 2.0, this list is stored on the Sametime home server you are assigned to. Each unique user ID that logs in has their own separate buddy list stored here. This allows each user to retrieve their own personalized list, no matter where they log in from.

Each user's list contains both ST and AOL entries.

5.13.1 Sametime buddies

Sametime 2.0 keeps your buddy list in a centralized database file (VPUSERINFO.NSF), stored on the home Sametime server, as assigned by the Sametime administrator. You can log in from any PC and access your personalized buddy list once you are connected to the Sametime community. Personalized nickname entries are also stored with the real names.

Do not attempt to edit user lists as stored on the VPUSERINFO.NSF file. Use the Connect client for all additions, changes, and deletions on your buddy lists.

If you are using a 2.0 client to access a 1.5 server, your buddy list will be stored locally as a DAT file in the Sametime directory. See the warning note below before you attempt to move this file onto a Sametime 2.0 server.

5.13.2 AOL buddies

AOL buddies are also stored on the server database (VPUSERINFO.NSF), intermixed with your Sametime names, in whatever order you have them sorted and entered. In your Connect buddy list, online AOL names will be distinguished by the AOL “running man” symbol (example in Figure 64) in your buddy list.

Figure 64. Close-up of Sametime Connect buddy list with AOL name indicator

Note that if you log into AOL without logging into Sametime, your user list will not be retrieved from the Sametime server. You will have an empty AOL list upon connection. Any names you add will be stored in a local file and not included in logins that do access the Sametime server. See the next section for an important note about merging list

5.13.3 Load list/Save list

You can load or save your buddy lists to and from a local file using the Connect client menu options. It is not possible however, to merge buddy lists together. When you load a new list, the list currently in use is over-written. Use the following menu selections from the Connect client to access the load and save list capability.

People -> Load List

People -> Save List

The lists are stored in a plain text file when stored locally. Once you have loaded them into your Connect client, they are moved onto the Sametime home server, in VPUSERINFO.NSF.

Attention

"Load List" WILL OVEWRITE ANY EXISTING LIST! There is no undo or way to back out. It would be better to refer to this option as "Overwrite List".

5.14 Connect preferences file

The **connect.ini** file is stored locally, and is common to all users of that PC. This means that all users of a single PC will share the same settings, preferences, and status messages. It can be edited with any text editor (such as Notepad). The values within are fairly self-explanatory, with option settings being 0=no, and 1=yes. Following is a sample of a connect.ini file.

```
[Login]
Server=sametime01.fishnet.com
User=Jim Kirk/Fishnet
Password=80,62,-124,-104,27,-48,-117,27,67,155,58,13,84,33,83,25,
AutoLogin=1
Server Port=1533
AppShare Port=8081
Proxy Type=0
Proxy Host=
Proxy Port=
Socks Type=0
Proxy User Name=
Proxy Password=
AOL ScreenName=SametimeTest
AOL Password=
AOL Autologin=0
KeepAliveTime=0
ResolveLocaly=0
[Aim Connectivity]
User Name=SametimeTest
Password=
Server Host=login.oscar.aol.com
Server Port=5190
Proxy Type=0
Proxy Host=
Proxy Port=1080
Socks Type=0
Proxy User Name=
Proxy Password=
Auto Login=0
[Setting]
```

```
WindowSize=747,68,1010,699
AlwaysOnTop=0
ShowActiveMessage=1
ShowAwayMessage=1
ShowDndMessage=1
LoginBlink=0
LoginSound=0
MessageBlink=1
MessageOnTop=1
MessageSound=1
ShowAddMessage=1
WarnUnsecuredMessages=1
ConversationMessage=Chat time!
AppShareMessage=Time to see what I am doing!!
ShowChangeStatus=1
ShowAll=0
ShowSorted=1
ShowShortNames=0
ShowSaveReminder=0
StatusBar=0
[ActiveMessages]
Message1=I AM ACTIVE
Message2=I live on this stuff - Sametime
Message3=I am online and working!
Message4=
Message5=
Message0=I am Here - or so you think
[AwayMessages]
Message1=Out to Lunch
Message2=Stepped out for a minute
Message3=Just at a meeting
Message4=
Message5=Out to Lunch
Message0=Gone!
[DNDMessages]
Message1=
Message2=Do not disturb me right now
Message3=Do not disturb me anytime
Message4=
Message5=
Message0=On an important call. Send email.
[Sounds]
Logon=C:\PROGRA~1\Lotus\SAMETI~1\BuddyIn.wav
Message=C:\WINNT\Media\Utopia Exclamation.WAV
[Timer]
ChangeStatus=15
SetTimer=1
```

```
AutoActive=1
[AudioVideo]
Microphone=0
Speaker=0
Video=0
[StartUpWindows]
ShowMyAvailableToolsDlg=1
ShowAudioVideoWizard=0
ShowAimDlg=0
```

Note: In the [message] lists, the message in the Message0 value is the one that will be displayed by default.

If you plan to have multiple users on a Connect client, do not use the “automatically log me on” feature. It can only store one password, and this would allow you to log on as the previous user.

If you are migrating a user from PC to PC, moving this file into the Sametime install directory will restore all preferences that existed before.

This file must be in the Sametime directory.

5.15 Client protocols

The following is a short explanation of the different protocols used by the Sametime clients to access each Sametime service.

- HTTP

  HTTP on port 80 is used to access the Sametime Web pages (either with or without Domino R5). This port is also used to download Java applets for meeting services to start.

- MCS (Multipoint communications services) on port 8081

  This is the port used for the T.120 protocol to transmit whiteboard and application sharing data between all participants in a meeting.

- MMCU/MMP (Multimedia Multipoint Control Unit/Muti Media Processor)

  This protocol controls the audio and video flows for both 2-way and 1-way transmissions. This protocol is a negotiated TCP or UDP port, with a fallback of TCP 8084.

- Community

  Community provides Virtual Places (awareness services). This uses port 1533 to transmit and receive data need to indicate online status to the Sametime servers, and for carrying instant message text.

Note: The Sametime client provides a direct link to America Online Instant Messenger (AIM) via port 5190. This connection does not route through any Sametime servers and it is directly dependent on your network's access to the Internet. This may require firewall configuration to allow a stable connection.

- Broadcast gateway

  This provides one way data for audio/video broadcasts. It uses tcp port 554 to negotiate the connection to the gateway, and then to specify whether to use a unicast or multicast protocol to transmit to the client.

- H.323 Clients

  Any H323 client (NetMeeting) can use a negotiated set of connections on TCP port 1720 and initiated H.245 call control.

If all users in a meeting are Net Meeting users, you can hold an interactive meeting with all services offered by Net Meeting.

5.16 Sametime multimedia equipment notes

A wide range of sound cards, microphones, and video cameras will work with Sametime. As there are too many to accurately list, we offer some general recommendations.

- **Sound cards**

  Use full duplex cards. A half-duplex sound card will not be able to use the automatic microphone mode in audio services. The reason is that it would be unable to detect the incoming and outgoing voice activity. Check your sound card manufacturer's specifications to deterime if you are full- or half-duplex. Most PCs and laptops manufactured in the past 3 years have full duplex.

- **Microphone**

  Use a high quality microphone and make sure you use a foam cover - it really helps cut out wind noises. A good boom microphone/headset comination is best, and they are not very costly. Ones with noise cancellation features are even better. Built-in microphones in laptops are prone to feedback, but will work.

- **Video**

  Do not try to use parallel port cameras. The feed is simply too slow, and the interface to the Windows video API is prone to problems. USB or PCMCIA connected cameras are best.

During our own testing, we used:

- IBM ThinkPad 600, 600E, T20
- IBM PC 300GL desktops
- Andrea Communications PC Headset (ANC 500) - ThinkPads required a ‘Thinkpad’ adapter jack for the microphone to be enabled. Thinkpad laptop speakers and microphones worked, but were very prone to a feedback problem if you had the speaker volume turned up.
- Intel PC Camera - with USB connections
- IBM UltraPort Camera (on T20 latop only)
- Windows 95 (client only), Windows NT 4.0 Server, Windows 2000 Professional, and Windows 2000 Server.

Chapter 6. Deploying Sametime on the Internet

In this chapter we outline a network topology and firewall configuration that allows users from the Internet to attend Sametime meetings with users on a corporate network behind a firewall.

Our implementation will be performed for Fishnet, a company that desires the full functionality of Sametime to be available to users from the Internet. Fishnet currently uses Lotus Notes and Lotus Domino for e-mail and workflow applications.

If you are new to firewalls, read this chapter from start to finish. If you are an experienced firewall administrator, refer to the network topology diagram in Figure 65 on page 151 and to our firewall ports quick reference in 6.4.3, “Quick reference of firewall settings” on page 164.

6.1 Determine the functionality first

The key to a successful Internet deployment is to decide up front what you need Sametime to do; that is, does your organization require chat and awareness across the Internet, do you want to have audio conferences with suppliers or partner organizations across the Internet, or would you like to run broadcast presentations on new products? The functionality you require will determine your firewall configuration.

Running a secure system is a trade-off between usability and security. The most secure of systems is locked in a dark room and switched off, which is not very usable or practical.

With this in mind, it is essential that you first decide how you can use Sametime in your organization from a business perspective. Once you have your purpose defined you can then look at how this will affect your firewall policy.

Understanding the trade-off between the business value and the risk of opening up a particular section of your firewall will help you decide if you want to go ahead and deploy a particular function of Sametime across the Internet.

Fishnet requires the following functionality:

1. Users on the Fishnet internal network can meet with each other using Community Services, Meeting Services, and audio/video.

2. Internal users can also initiate meetings that use Community Services, Meeting Services, and audio/video with known Internet users.
3. Internal users can initiate broadcast meetings that can be attended by internal users and Internet users.
4. Internet users can initiate broadcast meetings that can be attended by internal users and other Internet users.
5. The ability to split the load of Meeting Services and Community Services between internal and external users.

With these goals in mind, we can now decide the ports that need to be opened up on our firewall. This is discussed in 6.4.1, “Configuring the internal firewall” on page 152. However, before we get into a discussion about firewalls, we need to define some of the terms we will be using and look at the network environment that this solution will be deployed into, which is outlined in 6.3, “Network topology” on page 150.

6.2 Firewalls and the DMZ

DMZ is an internetworking term that comes from the military term “Demilitarized Zone,” meaning an area between two opponents where fighting is prevented.

When used in networking jargon, a DMZ refers to an area of a network, usually between two firewalls, where users from the outside are permitted limited access over a defined set of network ports and to predefined servers or hosts. A DMZ is used as the boundary between the Internet and a company’s internal network. It is the only place on a corporate network where Internet users and internal users are allowed at the same time.

A firewall is a system or group of systems that provide some form of access control between two networks. A firewall monitors all incoming and outgoing network traffic. This traffic must conform to certain rules. If a rule is not matched, the traffic will not be let through.

6.3 Network topology

Fishnet currently operates a secure network that sits behind 2 firewalls and a DMZ. The small boxes in the diagram represent network interface cards (NICs). Notice that each firewall has 2 NICs, and each NIC is plugged into a different IP network. Refer to Figure 65 on page 151.

Both of our firewall machines are running IBM Secureway Firewall 4.1 on Windows NT Server 4 with Service Pack 6.

Our traffic flow diagrams use the same terminology that is used inside IBM Secureway Firewall. These diagrams will aid in the setup of the rules under that particular tool. The first of these diagrams appears in Figure 66 on page 154.

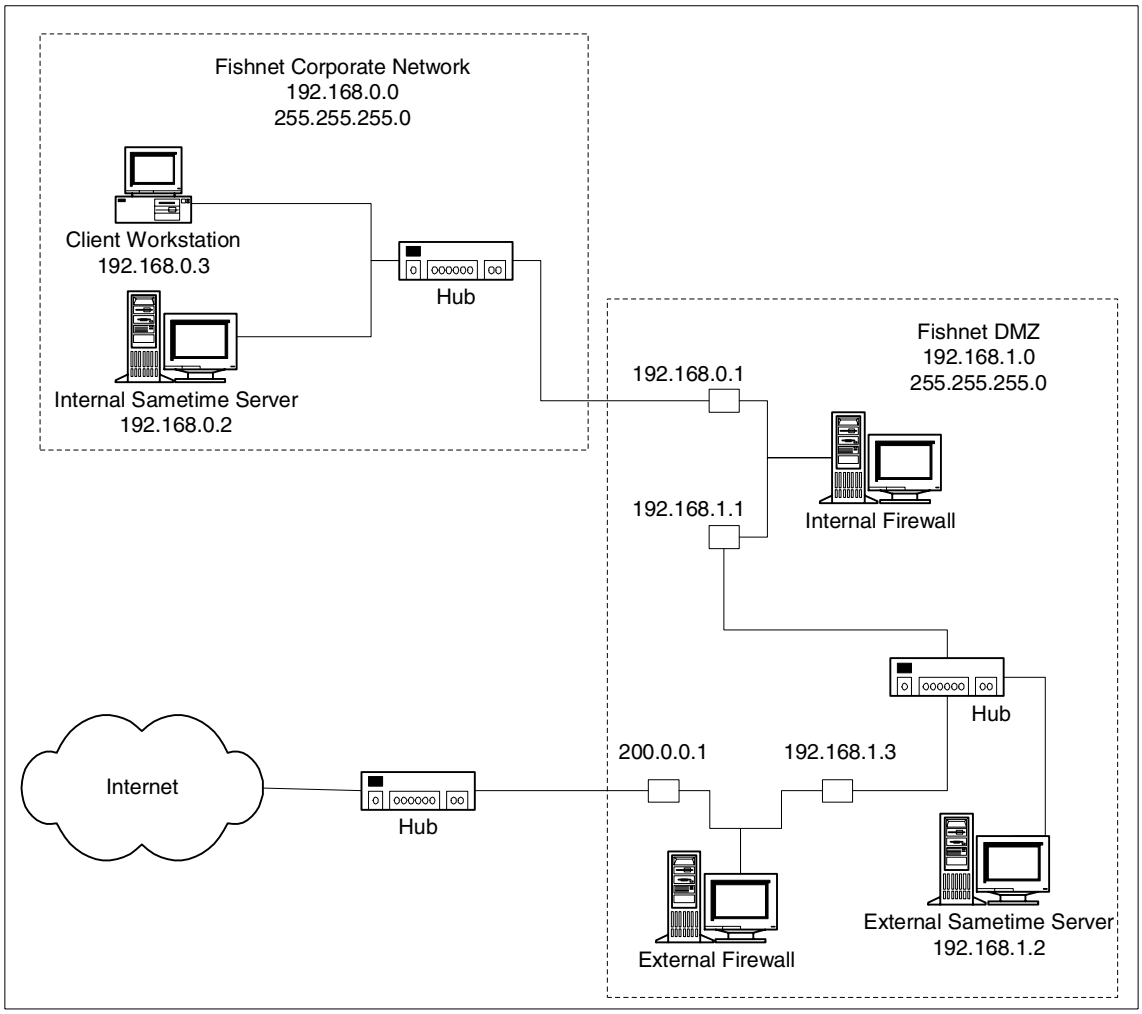


Figure 65. Fishnet's network topology

6.4 Firewall Configuration

The network topology in Figure 65 on page 151 has two firewalls, an internal and an external firewall. The ports opened up on each firewall are discussed in detail in this section.

6.4.1 Configuring the internal firewall

The first step in configuring the IBM Secureway Firewall is to define the objects that appear on your network. This requires a good knowledge of IP addressing concepts, including subnetting by using subnet masks. A discussion of this topic is beyond the scope of this redbook. Refer to *TCP/IP Tutorial and Technical Overview* GG24-3376 for a detailed discussion on this topic.

You should also note that this section assumes that the external firewall is configured correctly to allow the scenarios we present below. Detailed information on configuring ports on the external firewall can be found in the previously referenced redbook.

The network objects listed in Table 17 exist within the Fishnet Network and the DMZ.

Table 17. Network objects defined on the Fishnet internal firewall

Network Object Name	IP Address	Mask
Fishnet Corporate Network	192.168.0.0	255.255.255.0
Internal Sametime Server	192.168.0.2	255.255.255.255
Secure NIC	192.168.0.1	255.255.255.0
Non Secure NIC	192.168.1.1	255.255.255.0
Fishnet DMZ	192.168.1.0	255.255.255.0
External Sametime Server	192.168.1.2	255.255.255.255

Network objects allow the firewall administrator to tightly control the actual devices between which traffic is allowed to flow. Rules are used to further refine the type of traffic that travels between network objects. For example, a firewall rule may state that only TCP (Transmission Control Protocol) can flow between the internal and external Sametime servers on port 5000.

According to our list of desired functionality (6.1, “Determine the functionality first” on page 149) our first goal is to allow users on the Fishnet Corporate Network to participate in meetings that utilize Community Services, Meeting

Services and audio/video components of Sametime. This will work and require no firewall configuration since all of those users are on the same internal network. All users must attend on the internal Sametime server.

To achieve our remaining goals, a series of ports must be opened up on the internal firewall. These are detailed in the following sections.

6.4.1.1 Enabling HTTP traffic for Web browsers

In addition to Sametime-specific traffic, we want to allow our users to browse different Web servers on the Internet, so we open up port 80 from our internal network outbound. This comes in handy later on, when users on our internal network would like to directly schedule meetings on the external Sametime server or when the Sametime Administrator has a need to configure and monitor the external Sametime server using the browser-based Sametime Administration tool. We are currently not using an HTTP proxy in our DMZ. This is an option for future expansion.

6.4.1.2 Enabling Community Services

Community Services uses the TCP port 1516 for server-to-server connections. This port is required to enable the Community Services of the two Sametime severs to exchange presence and chat data and to perform directory updates.

Currently, our internal firewall allows outbound TCP traffic on port 1516 originating from the internal Sametime server going to the external Sametime server. The external Sametime server is also permitted to send TCP traffic back to the Sametime server on port 1516.

Figure 66 on page 154 summarizes the traffic flow on TCP port 1516.

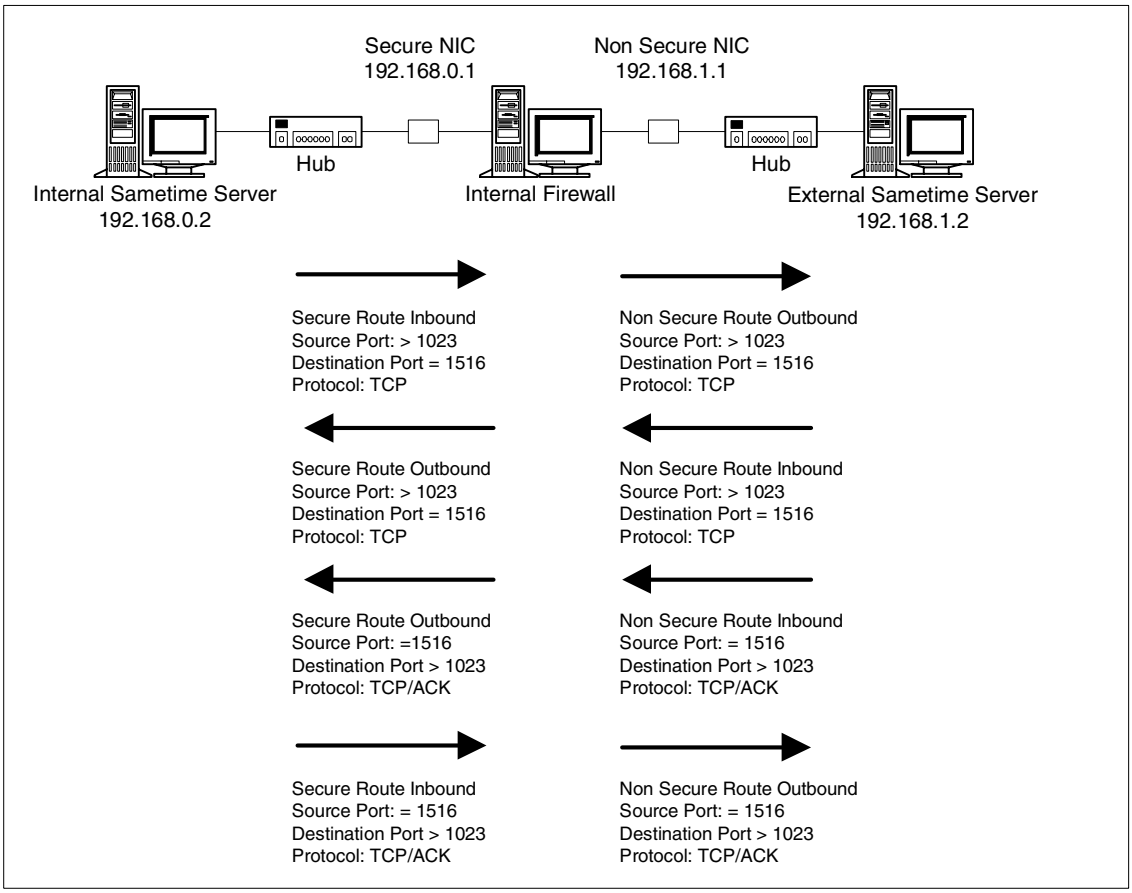


Figure 66. Traffic flow over TCP port 1516

We must also configure the firewall to receive TCP/ACK packets. The TCP protocol is a connection-oriented, end-to-end reliable protocol and as such it guarantees the delivery of data. The *ack* is used to acknowledge receipt of this data. If the sending station does not receive the ack within a given timeout period, the data is retransmitted. Refer to RFC 793 for details.

At this stage of our firewall configuration, internal users are still very much separated from external users.

Opening TCP port 1516 enables both servers to share presence and chat information only.

6.4.1.3 Enabling meeting services

Meeting services uses TCP port 1503 for whiteboarding and application sharing. Opening up port 1503 also allows Sametime meetings to start simultaneously across multiple servers via the T.120 protocol, for example. It will now be possible for the internal Sametime server to invite the external Sametime server to a meeting. Figure 67 summarizes the traffic flow over port 1503.

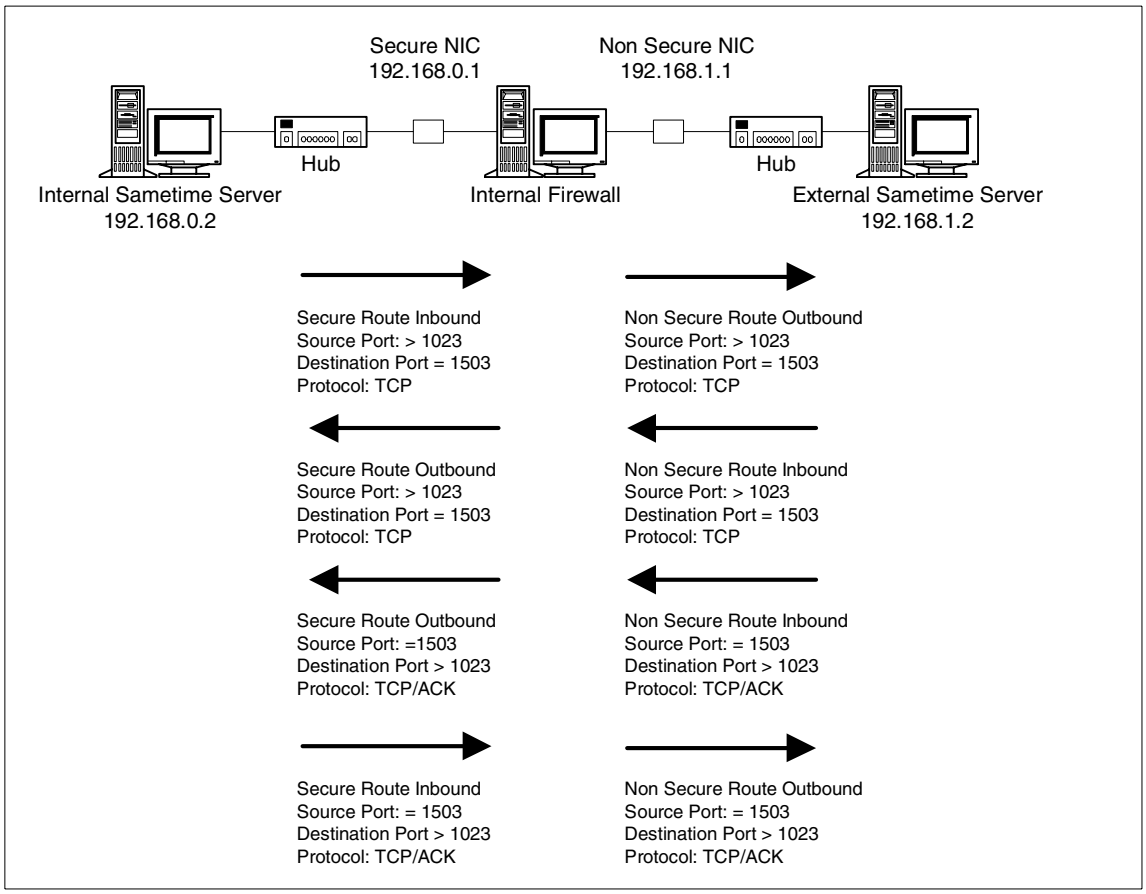


Figure 67. Traffic flow over TCP port 1503

When using invited servers, the load of the entire meeting is split across both the internal and external Sametime servers. Users attending on the external server can draw and post pictures on the whiteboard; this will all be processed on the external server and then transmitted to the internal server. This is discussed in more detail in the following section.

6.4.1.4 What have we achieved so far

Currently, TCP traffic is allowed to flow bi-directionally between the internal Sametime server and the external Sametime server on ports 1503 and 1516.

With these ports open, users attending on the internal Sametime server can meet with users attending on the external server and vice versa. Currently, these users have access to all functions of Sametime 2.0 except audio/video.

At this stage we have also achieved our fifth goal of splitting the load of meeting and community services between internal and external users. This works in the following manner:

1. An internal user initiates a meeting on the internal server and selects the option to allow external users to attend.
2. A T.120 broadcast is sent to the external Sametime server over port 1503.
3. The meeting appears in the external Sametime server's active meeting list in the Sametime Meeting Center.
4. Users on the Fishnet Corporate network log on to the internal Sametime server to attend the meeting.
5. Users attending from the Internet authenticate with the external Sametime server to attend the meeting.
6. When a user performs an action such as drawing on the whiteboard, it is processed on the server they have connected to and then transmitted to the other server participating in the meeting. For example, if an internal user puts a diagram on the whiteboard in the Meeting Room Client, this action will be processed by the internal Sametime server and transmitted to the external Sametime server, where the users attending the meeting on the external server will see the diagram.

The biggest advantage of using invited servers to distribute user load is a reduction in network bandwidth utilization. For example, if two users are attending on different invited servers, one copy of data travels over the WAN and is then distributed to all clients at the most local point. Refer to "Advantages of using multiple Sametime servers" in the Sametime Administrators Guide for more details. See also 2.4.2, "Multiple Sametime servers" on page 33.

6.4.1.5 Enabling interactive audio/video

To provide audio/video support for external and internal users, we need to open up port 8084 outbound from the internal firewall.

When using invited servers, audio/video cannot be distributed in the same way as application sharing and whiteboard. For example, if an interactive audio/video meeting is initiated on the external Sametime server and the internal Sametime server is invited, internal users can (and in fact should) attend that meeting on the internal Sametime server. Their Sametime Meeting Room client (MRC) will then connect to the internal Sametime server in order to get access to Community services and Meeting services. To send and receive the audio/video streams, however, their client automatically connects to the external Sametime server where the meeting was initiated.

The client attempts this audio/video connection on UDP ports first. Since we don't allow UDP traffic through our internal firewall, it falls back to tunneling the audio/video streams through TCP port 8084. Port 8084 must be open on all firewalls between the client and the server for audio/video transmission to be successful. Happily, we don't have to open an inbound connection on port 8084 from the DMZ to our internal network, as audio/video data is received via TCP/ACK packets. Figure 68 summarizes the traffic flow over port 8084.

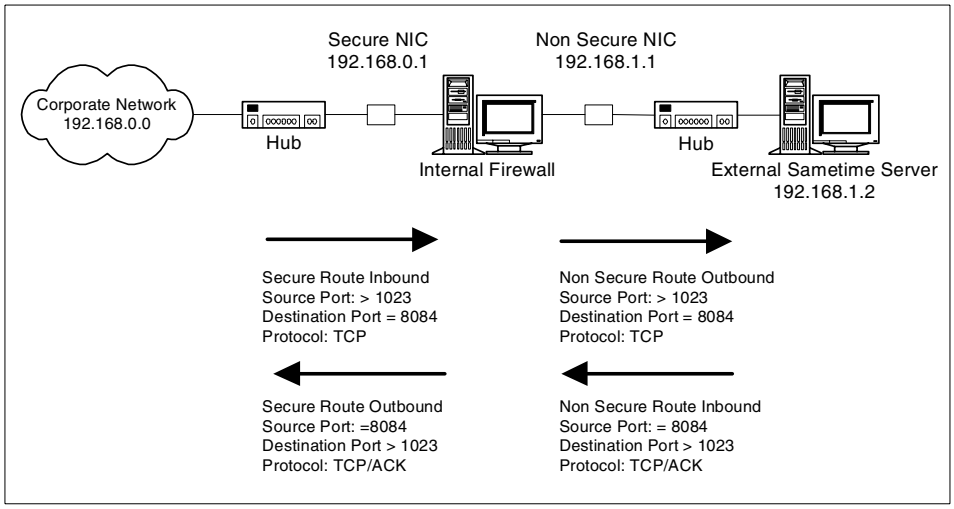


Figure 68. Traffic flow over TCP port 8084

6.4.1.6 Enabling broadcasting

Currently, our configuration has met all of the goals we listed in 6.1, "Determine the functionality first" on page 149. The final thing we need to enable is broadcast meetings.

We have enabled an outbound connection on port 554. This is so internal users can receive broadcast meetings that are being presented by known

internet users. This means that Fishnet's suppliers can log on and give presentations including audio/video to users on Fishnets internal network.

The way this will work under our current firewall configuration is as follows. The Broadcast client first performs a direct RTSP call control connection to the Broadcast Gateway over TCP port 554. Since our firewall does not allow UDP traffic, the broadcast meeting streams for audio, video and data are then tunnelled to the Broadcast client over port 554 using the RTSP TCP/IP connection, that was set up during the connection process. Figure 69 summarizes the traffic flow over port 554.

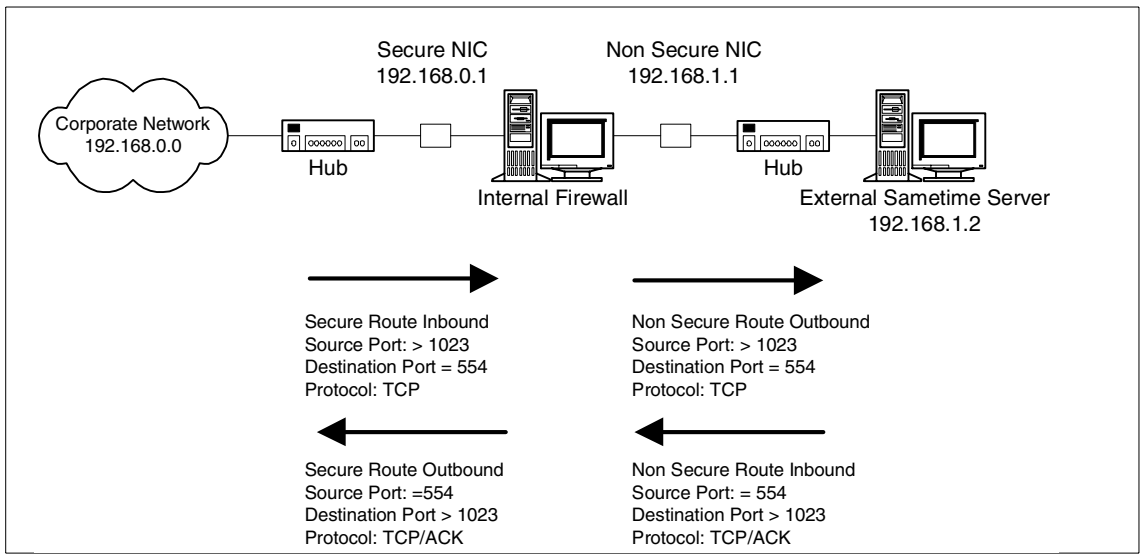


Figure 69. Traffic flow over TCP port 554

6.4.1.7 Enabling Notes and Domino connections

In addition to the Sametime-specific ports, we also opened up the internal firewall on port 1352 to allow for NRPC traffic (Notes remote procedure calls) between the internal network and the external Sametime server. There are several reasons to do this:

1. Both Sametime servers need to replicate some common Domino databases. For example, they're sharing the same directory information.
2. Our Sametime Administrator needs to access the Sametime server from their Notes Administrator client from time to time in order to do real time monitoring of Domino-specific tasks.

3. We are using the Domino event monitoring system on our Sametime servers. For example, we have set up an event monitor so that these servers automatically send an e-mail message to the administrator once the remaining free disk space falls under a predefined threshold value. In order for the external Sametime server to send such a message over the Domino mail routing protocol, port 1352 must be open. Figure 70 shows the TCP traffic flow on port 1352 between the internal network and our Sametime server in the DMZ.

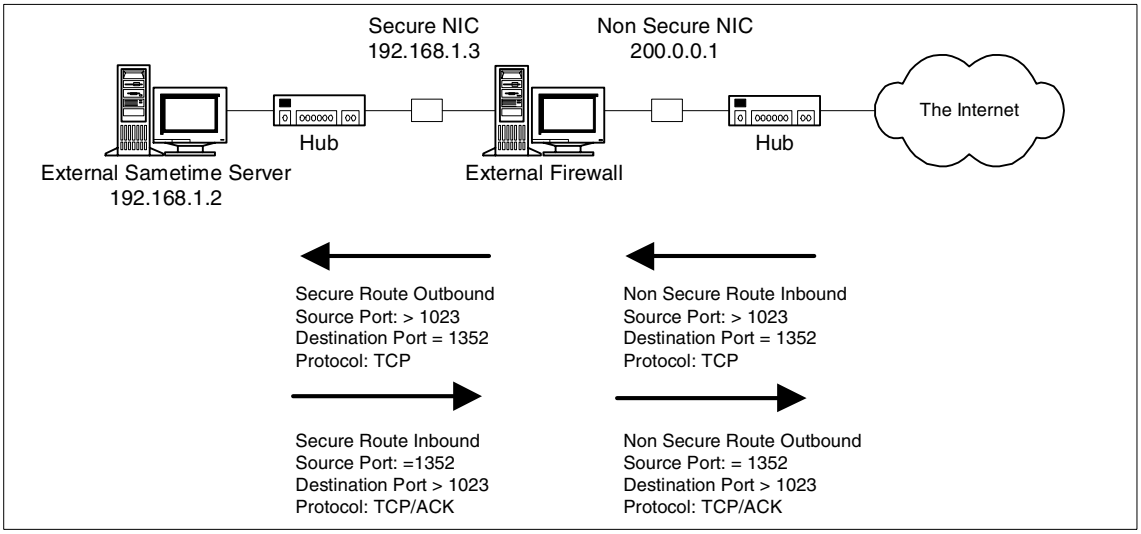


Figure 70. Traffic flow over TCP port 1352

6.4.2 Configuring the external firewall

Just like we did with the internal firewall, we begin the configuration of the external firewall by defining the necessary network objects.

The external firewall knows about the network objects listed in Table 18.

Table 18. Network objects known to the Fishnet external firewall

Network Object Name	IP Address	Mask
Fishnet DMZ	192.168.1.0	255.255.255.0
Secure NIC	192.168.1.3	255.255.255.0
Non Secure NIC	200.0.0.1	255.255.255.0
External Sametime Server	192.168.1.2	255.255.255.255
The Internet	0	0

Referring back to our list of requirements in 6.1, “Determine the functionality first” on page 149, we have to open up the external firewall so that users coming in over the Internet get access to Community Services, Meeting Services, and audio/video, as well as Broadcast Services. In addition to these Sametime-specific services, we also need to authenticate people and give them access to the conferencing database so that they can set up and attend meetings on the external Sametime server.

6.4.2.1 Enabling Web browser access

The external Sametime server’s HTTP service runs on port 80, so we have to open up the external firewall for inbound traffic from the Internet to the external Sametime server on that port.

As with the internal firewall, we must also set the external firewall to pass through TCP/ACK packets from the Sametime server in the DMZ back to the outside world.

Figure 71 shows the TCP traffic flow on port 80 between the Internet and our Sametime server in the DMZ.

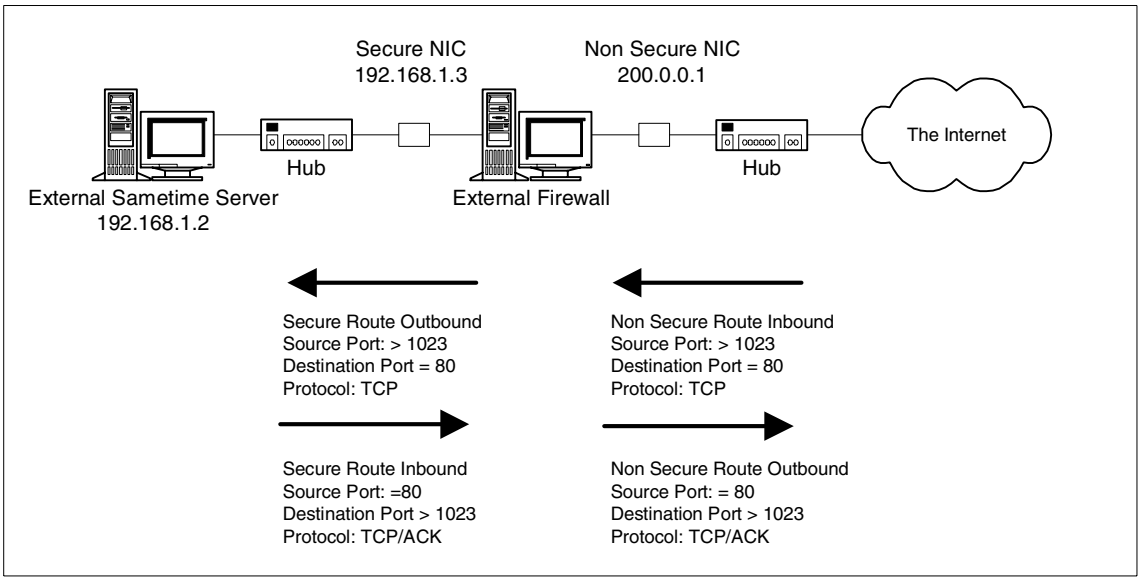


Figure 71. Traffic flow over TCP port 80

With port 80 open, external users can now authenticate with the external Sametime server. Assuming they have been given appropriate access rights

to the conferencing datase, they can now see a list of meetings and also create new meetings on the external Sametime server.

The next step is to further open up the external firewall so that external users can also attend meetings on the external Sametime server. As we've done with the internal firewall setup, we're now going to enable access to Community Services, Meeting Services, audio/video and Broadcast Services.

6.4.2.2 Enabling access to Community Services

The external Sametime server is set so that Community Services listen for client connections coming in via HTTP tunneling requests over port 8082.

We decided not to open up the default Community Services client port 1533 because we don't expect external Sametime Connect users connecting to our external Sametime server using a direct TCP/IP connection. Opening up port 8082 to access Community Services via HTTP tunneling also allows external users to connect to our Sametime Community using the Java Connect client or using the Sametime Connect client when sitting behind their company firewall accessing the Internet through an HTTP proxy. For more information about the connection process to Community Services, see 4.2.2.1, "Sametime Connect client connection process" on page 97. Figure 72 summarizes the traffic flow over port 8082.

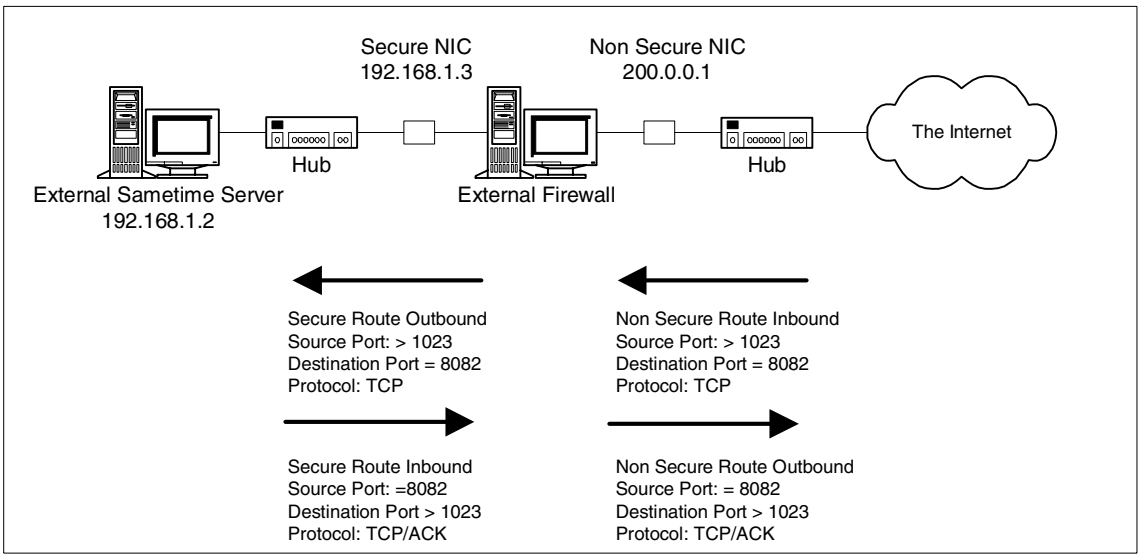


Figure 72. Traffic flow over TCP port 8082

6.4.2.3 Enabling access to Meeting Services

Meeting Services listen on port 8081 for client connections. By opening up this port, people are now able to attend and interact in meetings that include the chat, shared whiteboard, and screen-sharing tools.

Figure 73 shows the TCP traffic flow over port 8081.

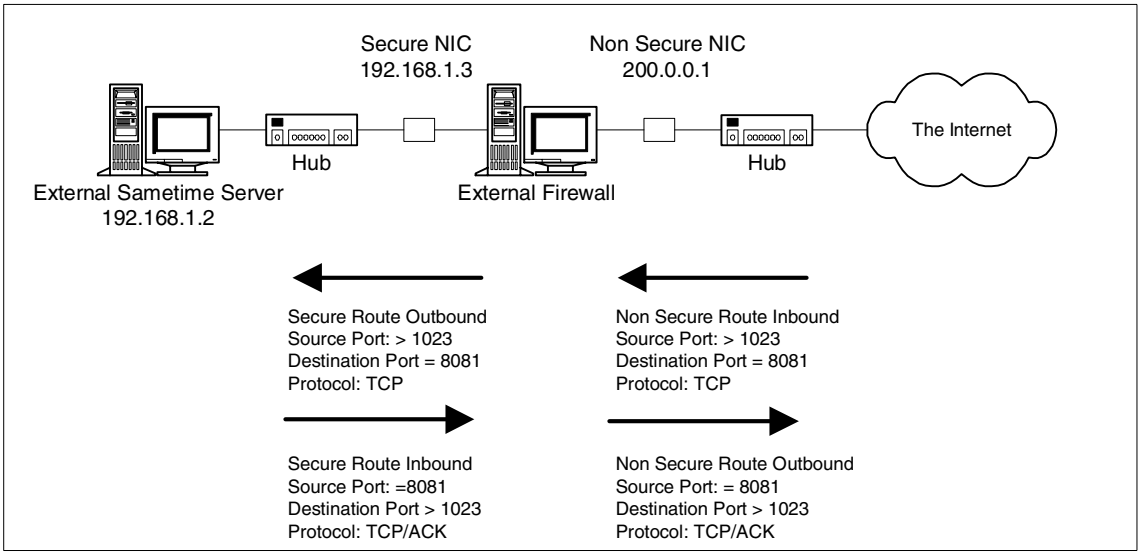


Figure 73. Traffic flow over TCP port 8081

With ports 80, 8081 and 8082 opened up so far, external users can now create and attend interactive Sametime meetings containing the basic set of tools (Meeting Room Chat, Whiteboard, ScreenSharing). These meetings can be restricted to other users attending on the external Sametime server. In addition, they can also be extended to include users attending the same meeting on Fishnet's internal Sametime server simply by inviting the internal server when the meeting is created.

The next step is to configure the firewall to allow for interactive audio/video meetings.

6.4.2.4 Enabling interactive audio/video

To provide interactive audio/video support for external users, in addition to port 8081, which is already open, we now need to open up the external firewall so that the Sametime meeting room client running on an external user's machine can send and receive audio/video streams. The default way to send and receive these streams would be via randomly selected UDP ports

out of a predefined range. We decided not to open up our external firewall for UDP traffic; instead, we used the already described fall back method for TCP tunneling. Therefore, we have to open up TCP port 8084 inbound between the Internet and the external Sametime server.

Figure 74 shows the TCP traffic flow over port 8084.

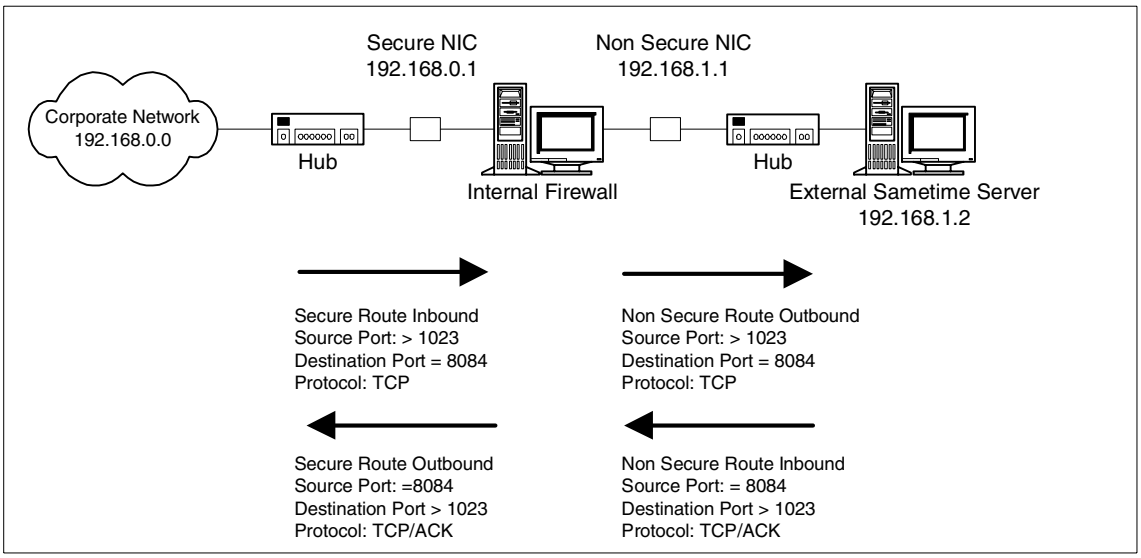


Figure 74. Traffic flow over TCP port 8084

Just as with the other ports, port 8084 must be open on all firewalls between the client and the server for audio/video transmission to be successful. This must be taken into consideration if any external user connects to our Sametime server via their company firewall or any other proxy server.

6.4.2.5 Enabling Broadcast Meetings

The last step is to configure the external firewall to allow for attending Broadcast meetings from the Internet. The Broadcast Gateway on the external Sametime server is set to listen for direct client connections on port 554. It also listens for incoming HTTP tunneling connections on the very same port.

An external user with a direct Internet connection downloads the Broadcast Client over http port 80 and then performs a direct RTSP call control connection to the Broadcast Gateway over TCP port 554. Since our firewall does not allow UDP traffic, the broadcast meeting streams for audio, video, and data are then tunnelled to the Broadcast client over port 554 using the

RTSP TCP/IP connection that was set up during the connection process. The same is true for someone connecting to the Internet via a SOCKS server.

An external user behind a company firewall, who has to connect to the Internet over their company's HTTP proxy server, would also download the Broadcast Client over http port 80. They would then set up the RTSP call control connection to the Broadcast Gateway via HTTP tunneling over port 554. Finally, the broadcast streams would then sent to the Broadcast client over port 554 via HTTP tunneling using the existing RTSP connection.

Figure 75 summarizes the traffic flow over port 554.

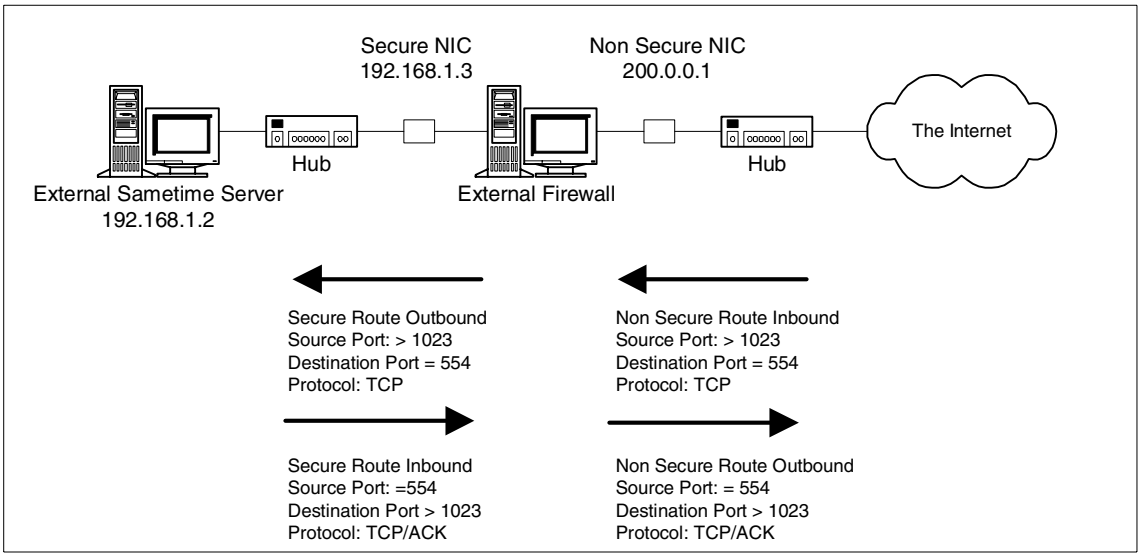


Figure 75. Traffic flow over TCP port 554

6.4.3 Quick reference of firewall settings

Fishnet's business goals, outlined at the beginning of this chapter, drive the requirements for the following firewall settings. For an overview of Fishnet's network topology, refer to the diagram in 6.3, "Network topology" on page 150.

Note

For all TCP ports that have been opened up on the firewalls, you must also remember to set the firewall so that the corresponding TCP/ACK packets can travel back from the target to the originating source systems. For more details, see the Community Services example in 6.4.1.2, “Enabling Community Services” on page 153.

Besides TCP and TCP/ACK packets, both firewalls are closed for any other type of traffic. Although technically possible, they also do not run any type of proxy software (SOCKS, HTTP proxy, and so forth).

6.4.3.1 Summary of internal firewall settings

Table 19 is a quick summary of the open TCP ports on the internal firewall.

Table 19. Fishnet iInternal firewall settings

TCP Port	Direction	Between	and	Reason
80	outbound	Fishnet Corporate Network	Fishnet DMZ	Web browser traffic
554	outbound	Fishnet Corporate Network	External Sametime Server	Broadcast Service RTSP / RTP
1352	both	Fishnet Corporate Network	External Sametime Server	Notes and Domino NRPC
1503	both	Internal Sametime Server	External Sametime Server	Meeting Services
1516	both	Internal Sametime Server	External Sametime Server	Community Services
8084	outbound			interactive audio video RTCP / RTP

6.4.3.2 Summary of external firewall settings

Table 20 is a quick summary of the open TCP ports on the external firewall.

Table 20. Fishnet external firewall settings

TCP Port	Direction	Between	and	Reason
80	outbound	The Internet	External Sametime Server	Web browser traffic
554	outbound	The Internet	External Sametime Server	Broadcast Service RTSP / RTP
8081	outbound	The Internet	External Sametime Server	Meeting Services
8082	outbound	The Internet	External Sametime Server	Community Service HTTP tunneling
8084	outbound	The Internet	External Sametime Server	interactive audio video RTCP / RTP

It is worthwhile noting here, that while the above firewall is extremely secure, the trade-off is that it is inefficient.

6.5 Directory and security considerations

Driven by the business requirements outlined at the beginning of this chapter, Fishnet discovered that they had to make decisions about several directory and security-specific topics. This section describes their considerations and solutions.

6.5.1 Managing directory information

Fishnet decided to keep directory information for external customers and suppliers separate from their internal users directory. The primary purpose of Fishnet's external Sametime service is to support dedicated business contacts. Due to the dynamic nature of the market, they need to get in touch with new customers and prospects as quickly as possible. That's why they did not want to rely on the IT department to manage their directory of external contacts. Instead, they wanted dedicated line of business people to have authority over the information describing their customers and suppliers.

Fishnet also has a large number of sales reps traveling all over the world. They usually dial up the nearest ISP to get Internet connectivity. While on the road, they need to stay in touch with their managers back in the offices in

New York and Tokyo, as well as with their customers. So Fishnet decided that these types of users should also use the external Sametime service.

These requirements lead to the configuration described in the next section.

6.5.1.1 Using multiple directories with Directory Assistance

To separate internal and external directory information, Fishnet created a separate directory database (ExternalContacts.nsf) on one of their internal Domino servers. This database holds all external contacts, and dedicated line of business people have been given authority to create and modify person documents using their Notes clients or a Web browser. A replica copy of this database is available on the internal Sametime server.

In order to tell both Sametime servers about this secondary directory, Fishnet introduced Directory Assistance, a standard feature of Lotus Domino and, therefore, Lotus Sametime. Entries in the Directory Assistance database tell their Sametime servers where and how to find the external users directory. Fishnet decided to place a replica of the ExternalContacts.nsf database on both the internal and external Sametime servers, so the external Sametime server can access it when authenticating external users. Note that the external Sametime server could have also accessed a replica copy of that directory database directly on the internal server because the internal firewall is open for Notes NRPC traffic between both servers.

To enable Directory Assistance, we created a new Notes database on the Sametime server. This database should be based on the Directory Assistance template (da50.ntf). We named this database MAB.nsf. Then we told the Sametime server to use the information in this database by modifying the server document, as shown in Figure 76:

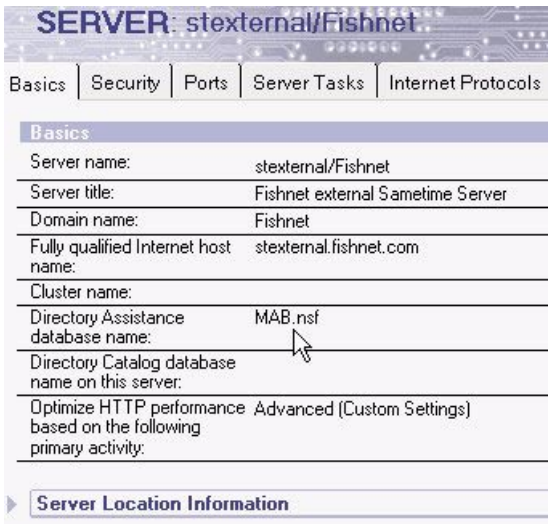


Figure 76. Entry in server document to enable Directory Assistance

The next step is to create a Directory Assistance document in the Directory Assistance database (MAB.nsf) to describe the secondary directory, which holds the person records for Fishnet's customers and suppliers.

Figure 77 and Figure 78 show the details concerning that document.

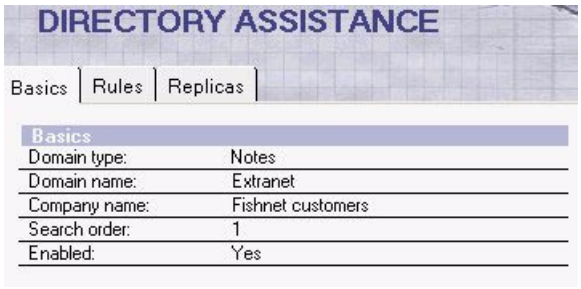
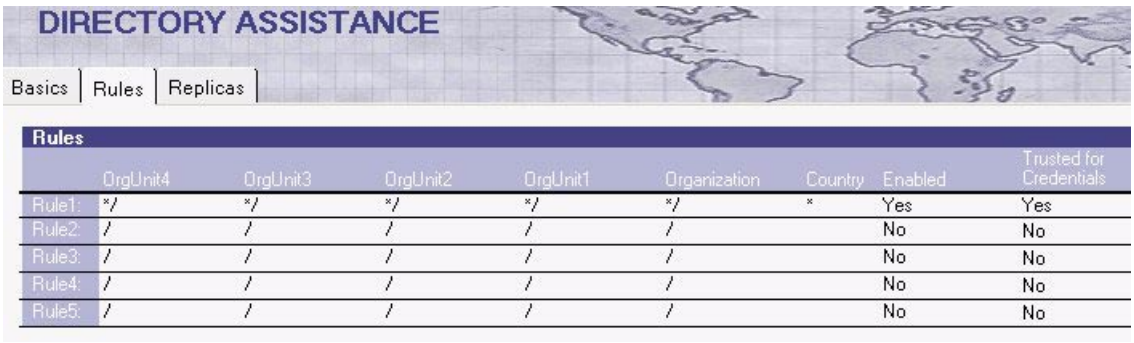


Figure 77. Basic settings in the Directory Assistance document

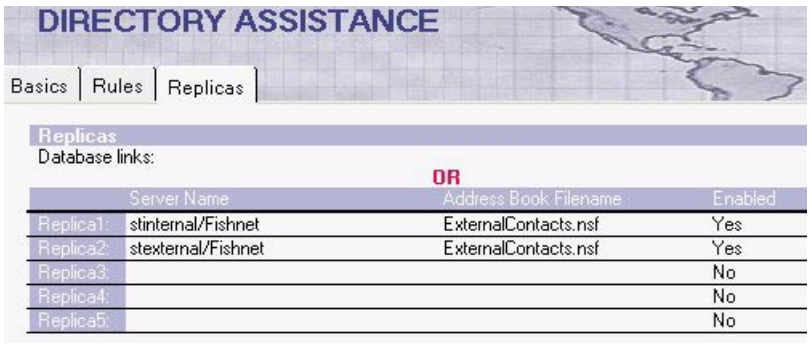


	OrgUnit4	OrgUnit3	OrgUnit2	OrgUnit1	Organization	Country	Enabled	Trusted for Credentials
Rule1:	*/	*/	*/	*/	*/	*	Yes	Yes
Rule2:	/	/	/	/	/		No	No
Rule3:	/	/	/	/	/		No	No
Rule4:	/	/	/	/	/		No	No
Rule5:	/	/	/	/	/		No	No

Figure 78. Rules settings in the Directory Assistance document

Note that this secondary directory is set to be trusted for credentials.

Finally, we have to tell the Sametime server where to find the directory. The illustration of this is in Figure 79 on page 169.



	Server Name	Address Book Filename	Enabled
Replica1:	stinternal/Fishnet	ExternalContacts.nsf	Yes
Replica2:	stexternal/Fishnet	ExternalContacts.nsf	Yes
Replica3:			No
Replica4:			No
Replica5:			No

Figure 79. Replica settings in the Directory Assistance document

For more information about Directory Assistance see the Domino Administrator's Guide.

6.5.1.2 Restricting access to the external Sametime server

Both Sametime servers and all internal Domino servers currently belong to the same Domino domain, so they all replicate the primary directory (usually called names.nsf). Fishnet did not want all of their employees to be able to use the external Sametime service, either over the Internet or from the company internal LAN. In addition to their customers and suppliers, they wanted this capability to be reserved for Fishnet's sales, marketing, and customer service divisions.

That's why they have set up selective replication of the primary directory between the internal and the external Sametime server, so that only person documents of Fishnet's employees from the sales, marketing, and customer service divisions end up in the replica on the external Sametime server. Explaining how to set up selective replication is beyond the scope of this book. See the Domino documentation for details.

Finally, Fishnet removed anonymous access and self-registration from both the internal and the external Sametime server. Again, the Sametime Administrator's Guide has detailed instructions on how to do this.

6.6 Summary of Fishnet's Sametime service

This section summarizes Fishnet's Sametime services, which are available to internal employees as well as customers and suppliers, after applying the firewall and Domino-specific configuration settings. It also describes how internal users create and attend different types of meetings.

6.6.1 Internal users

All Fishnet employees are *internal* users as long as they do not access the external Sametime server over the Internet.

6.6.1.1 Internal meetings

Fishnet employees on the company internal network can now create and attend all types of Sametime meetings on the internal Sametime server. Because we removed anonymous access and self-registration, they have to authenticate with their username and internet password in order to get access to any kind of Sametime conferencing capabilities. They can also use their Sametime Connect client and even include external customers and suppliers in their buddy lists, because the internal Sametime server uses the ExternalContacts.nsf database via Directory Assistance.

6.6.1.2 Meetings between internal and external users

If internal users want to have common interactive meetings together with external users (customers, suppliers, or their travelling colleagues from the sales department, for example), they simply create the meeting on the internal server and invite the external Sametime server at the same time. Internal users attend such meetings on the internal Sametime server only.

With the current firewall setup these types of distributed meetings must not contain audio/video capabilities because the server portion of the interactive

audio/video runs on the originating server only. In this case, that would be the internal server, and external users wouldn't get access to it.

If internal users need to run interactive meetings including audio/video, and attended by both internal and external users at the same time, they create these types of meetings on the external Sametime server first and invite the internal Sametime server. This capability to create such meetings on the external Sametime server is currently restricted to internal users from the sales, marketing, and customer service divisions because, due to our selective replication setup, the external Sametime server only holds person documents of internal users from these divisions.

The ability to attend these meetings, however, is available for all Fishnet employees because all internal users including the meeting creators attend these types of meetings on the internal Sametime server only. Under the covers, the Sametime Meeting Room client is smart enough to connect to Community and Meeting Services on the internal server and switch over to the external server for audio/video by tunneling through the firewall.

Finally, for broadcast meetings that should be attended by both internal and external users at the same time, the ability to create and attend such meetings is restricted to internal users from the sales, marketing, and customer service divisions because such meetings must be created and attended on the external Sametime server only. Otherwise, external users would not be able to get access to the broadcast streams. If Fishnet wanted all internal users to be able to create and attend such a broadcast meeting on the external server, they would simply make a full replica of the primary directory available on the external Sametime server.

6.6.2 External users

With the current directory setup, external users consist of Fishnet's customers and suppliers listed in ExternalContacts.nsf. If Fishnet employees from the sales, marketing, and customer service divisions access the external Sametime server over the Internet, they are also considered external users, although they are not listed in ExternalContacts.nsf.

Because we removed anonymous access and self-registration on the external Sametime server, everyone accessing that server has to authenticate using their username and internet password to get access to any kind of Sametime capabilities.

External users can now create and attend all types of Sametime meetings on the external Sametime server. When they want to run a meeting between

internal and external users, they simply invite the internal server while creating the meeting on the external server. Using Sametime Java Connect or (if they connect to Fishnet's external Sametime server via an HTTP proxy) using the Sametime Connect client, they can also include internal users in their buddy lists.

By opening up port 1533 inbound on the external firewall, any registered user could access Community Services on the external Sametime server directly, that is, without using the HTTP tunneling method. The Sametime Connect client can use the HTTP tunneling method only, when connecting through an HTTP proxy. The Sametime Java Connect client, however, can be set to directly use HTTP tunneling. For more information about Sametime Java Connect, see `http://www.lotus.com/sametime`

Note

By opening up port 1533 inbound on the external firewall, any registered user could access Community Services on the external Sametime server directly, that is, without using the HTTP tunneling method. The Sametime Connect client can use the HTTP tunneling method only, when connecting through an HTTP proxy. The Sametime Java Connect client, however, can be set to directly use HTTP tunneling. For more information about Sametime Java Connect, see http://www.lotus.com/sametime.

6.6.3 Reality check

As you have seen in the preceding sections, with our current firewall and directory-specific setup, it's quite complex for internal users to create and attend various types of meetings that include both internal and external users at the same time.

In fact, the internal users have to follow a certain set of rules:

- For internal-only meetings, they create and attend these meetings on the internal server only. No restrictions apply.
- For interactive meetings with external users, they create and attend these meetings on the internal server. These meetings, however, can not include audio/video or broadcast services.
- For interactive audio/video meetings with external users, they create these meetings on the external server, invite the internal server, and attend the meeting on the internal server.

- Finally, for broadcast meetings that include external users, they create and attend these meetings on the external server.

The reason we have implemented the Fishnet demo scenario that way is to show you the effect of the various techniques that are available. You should now understand:

- How firewall ports relate to the different Sametime services for both clients and servers.
- The benefits of running multiple Sametime servers.
- The importance of where to place a multimedia add-on and where to run a broadcast gateway.
- The flexibility and control you gain when using multiple directories, selective replication, and access control lists.

In a real world implementation, you would probably open up a few more ports on the internal firewall, so that for all meetings that must be held with external users, an internal users would just create and attend that meeting on the external Sametime server.

This concludes our description of Fishnet's implementation of Sametime services on the Internet.

Appendix A. Using the additional material

This redbook references additional Web material. The following sections describe how to locate and use this material.

A.1 Locating the additional material on the Internet

The Web material associated with this redbook is available on the Internet from the IBM Redbooks Web server. Point your Web browser to:

ftp://www.redbooks.ibm.com/redbooks/sg246206.zip

Alternatively, you can go to the IBM Redbooks Web site at:

ibm.com/redbooks

Select the **Additional materials** and open the directory that corresponds with the redbook form number.

A.2 Using the Web material

The additional Web material that accompanies this redbook includes the following:

File name	*Description*
sg246207.zip	Zipped Samples

A.2.1 System requirements for downloading the Web material

The following system configuration is recommended for downloading the additional Web material.

Operating System:	Windows/32
Processor:	Any
Memory:	Any

A.2.2 How to use the Web material

Create a subdirectory (folder) on your workstation and copy the contents of the Web material into this folder.

Appendix B. Special notices

This publication is intended to help network administrators and Sametime deployers to understand how Sametime works in a network environment, and how to best install, deploy and configure it for their own environment. The information in this publication is not intended as the specification of any programming interfaces that are provided by the Lotus Sametime product.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

IBM ®	Redbooks
Domino	Redbooks Logo 
Lotus	SP
Lotus Notes	SP2
Lotus Sametime	System/390
Notes	ThinkPad
Sametime	Wizard
SecureWay	400

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks

owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix C. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

C.1 IBM Redbooks

For information on ordering these publications see “How to get IBM Redbooks” on page 183.

- *Lotus Sametime Application Development Guide*, SG24-5651
- *Lotus Notes and Domino Take Center Stage: Upgrading from R4 to R5,* SG24-5630
- *Getting the Most from Your Domino Directory*, SG24-5986
- *TCP/IP Tutorial and Technical Overview,* GG24-3376-05
- *A Secure Way to Protect Your Network: IBM SecureWay Firewall for AIX V4.1*, SG24-5855-00
- *Lotus Notes and Domino R5.0 Security Infrastructure Revealed,* SG24-5341

C.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at ibm.com/redbooks for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
IBM System/390 Redbooks Collection	SK2T-2177
IBM Networking Redbooks Collection	SK2T-6022
IBM Transaction Processing and Data Management Redbooks Collection	SK2T-8038
IBM Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
IBM AS/400 Redbooks Collection	SK2T-2849
IBM Netfinity Hardware and Software Redbooks Collection	SK2T-8046
IBM RS/6000 Redbooks Collection	SK2T-8043
IBM Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

C.3 Other resources

- Sametime 2.0 Administrators Guide
- Sametime Installation Guide

These Lotus Whitepaper publications are also relevant as further information sources:

- *Sametime 2.0 Performance and Best Practices Whitepaper,* CC7R3NA
- *Getting Started with Sametime Audio and Video - Get up and running with Sametime's A/V capabilities*, CC7MENA
- *Sametime Multimedia Services Whitepaper - A more technical view of Sametime A/V capabilities*, CC639NA
- Lotus Sametime White Paper V1.0 9/28.1999
- “Real-time Collaboration Standards,” available on the web at `ftp://ftp.lotus.com/pub/lotusweb/product/sametime/ST_standards.pdf`

C.4 Referenced Web sites

This Web site is relevant as a further information source:

- `http://www.lotus.com/sametime/` The Lotus Sametime homepage.

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** ibm.com/redbooks

  Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the IBM Redbooks fax order form to:

	e-mail address
In United States or Canada	pubscan@us.ibm.com
Outside North America	Contact information is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

IBM Redbooks fax order form

Please send me the following:

Title	Order Number	Quantity

First name	Last name	
Company		
Address		
City	Postal code	Country
Telephone number	Telefax number	VAT number

☐ Invoice to customer number _____

☐ Credit card number _____

Credit card expiration date	Card issued to	Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

Symbols

A

B

C

D

E

F

H

T

U

V

W

IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at **ibm.com**/redbooks
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Document Number **Redbook Title**	SG24-6206-00 Lotus Sametime 2.0 Deployment Guide
Review	
What other subjects would you like to see IBM Redbooks address?	
Please rate your overall satisfaction:	O Very Good O Good O Average O Poor
Please identify yourself as belonging to one of the following groups:	O Customer O Business Partner O Solution Developer O IBM, Lotus or Tivoli Employee O None of the above
Your email address: The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	O Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
Questions about IBM's privacy policy?	The following link explains how we protect your personal information. **ibm.com**/privacy/yourprivacy/

(0.2”spine)
0.17”<->0.473”
90<->249 pages

Lotus Sametime 2.0 Deployment Guide

Sametime 2.0 architecture and features

Networking and firewalls in depth

Deploying Sametime 2.0 within your organization and on the Internet

Lotus Sametime is a real-time collaboration tool that allows you to communicate with others instantly. Sametime 2.0 brings new features and functionality to the table, with the most notable being real-time audio and video. These exciting new features combine with the existing tools of real-time chat, conferencing, and application sharing, which were already available in the previous version of Sametime. Because of the wealth of features in the product, it is important to understand how Sametime 2.0 functions and what its impact will be before deploying it in your organization.

This IBM Redbook will help you install, tailor, and configure Sametime 2.0 to meet your business needs. It provides all the information you need to make decisions on how best to deploy Sametime 2.0. Specifically, this redbook describes the different installation options for Sametime, planning considerations, upgrading from Sametime 1.5, hardware recommendations, and performance considerations. A detailed look at the Sametime 2.0 architecture and components is provided, as well as descriptions of some of the exciting extensions to Sametime, such as Sametime for WAP and translation services. The different Sametime clients available are discussed, and an example of a real-world deployment of Sametime 2.0 between two companies over the Internet is presented.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6206-00 ISBN 0738419556